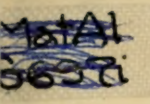

3 1761 07548285 1

INTRODUCTION

A LA THÉORIE DES

NOMBRES ALGÉBRIQUES



Dr J. SOMMER

PROFESSEUR A LA « TECHNISCHE HOCHSCHULE » DE DANTZIG

INTRODUCTION

A LA THÉORIE DES

NOMBRES ALGÉBRIQUES

Edition française revue et augmentée

TRADUIT DE L'ALLEMAND

PAR

A. LÉVY

PROFESSEUR AU LYCÉE SAINT-LOUIS

Avec Préface de J. HADAMARD

PROFESSEUR AU COLLÈGE DE FRANCE

PARIS

LIBRAIRIE SCIENTIFIQUE A. HERMANN ET FILS

LIBRAIRES DE S. M. LE ROI DE SUÈDE

6, RUE DE LA SORBONNE, 6

1911

PRÉFACE DE L'ÉDITION FRANÇAISE

L'école mathématique française du temps présent a-t-elle eu raison de laisser dans un oubli relatif la théorie des nombres pour s'adonner aux autres branches de la mathématique où, certes, elle a trouvé assez de problèmes à élucider et de résultats à recueillir pour alimenter son activité ?

C'est affaire à chacun de l'apprécier.

Que cet oubli soit réel — si étrange qu'il puisse paraître dans la patrie d'Hermite — il n'est même plus utile de le rappeler.

Parmi tous ceux — et leur nombre est respectable — qui, en France, s'intéressent aux mathématiques, combien connaissent les théories modernes de l'Arithmétique ?

Combien même, pourrait-on se demander, soupçonnent qu'au delà des théorèmes de Fermat et de Wilson existe toute une science, — j'entends une science cohérente, se développant avec autant de continuité et d'harmonie que les plus belles et les plus classiques théories de l'Analyse ?

Aussi cette science n'est-elle abordée qu'à de rares intervalles dans les travaux de nos chercheurs, si attirés aujourd'hui par l'Analyse, la Géométrie, la Mécanique. Je ne parle pas, bien entendu, de travaux où sont simplement collectionnés des faits sans relation entre eux et sans portée, formant aussi peu une science — pour reprendre un mot de M. Poincaré — qu'un tas de pierres n'est une maison, précisément parce qu'ils ne tiennent compte que des anciens points de vue dont l'intérêt est aujourd'hui épuisé et ignorent les aspects modernes de la question.

Cette ignorance a eu jusqu'ici une excuse : elle avait à la fois pour conséquence et pour cause l'absence de tout Traité et de tout enseignement français sur ces matières.

Nous pouvons compter que cette excuse va disparaître et que cette lacune sera comblée.

L'Université de Paris a tout d'abord ressenti la nécessité d'agir dans ce sens ([1]). Sous ses auspices, la Théorie des nombres est, dès maintenant, enseignée par un des mathématiciens qui, dans notre pays, ont le plus activement travaillé à ses progrès. La compétence reconnue avec laquelle cet enseignement est professé ne permet pas de douter qu'il ne porte ses fruits.

M. Lévy a voulu coopérer au même but.

Grâce à lui, on pourra bientôt, je l'espère, lire en français l'exposition la plus magistrale qui ait été tracée jusqu'ici de la Théorie des corps algébriques dans son état actuel, je veux parler de l'article inséré par M. Hilbert au *Jahresbericht der deutschen Mathematiker-Vereinigung* en 1895. Mais il a aussi pensé que l'œuvre si approfondie et si condensée du maître de Göttingue ne pouvait être abordée sans préparation et c'est à ce besoin qu'il a répondu en offrant au public français la traduction de l'ouvrage plus modeste et plus élémentaire de M. Sommer.

Ce n'est pas, d'ailleurs, que celui-ci ne conduise déjà fort avant et fort loin. Non seulement par l'exemple simple du corps quadratique, complété par celui du corps cubique, l'auteur tient et réussit à munir le lecteur de toutes les notions fondamentales et à lui faire constater toutes les circonstances importantes qui se présentent dans le cas général. Mais même, avec l'étude du corps relativement quadratique, par laquelle se termine le volume, et avec le curieux ensemble d'analogies et de différences qu'il manifeste lorsqu'on le compare aux corps considérés dans le domaine naturel, on sort nettement de la partie proprement élémentaire et classique de la théorie. C'est, en un mot, avec peu d'efforts, une vue fort complète de celle-ci qu'on acquiert en suivant M. Sommer.

Ces qualités me paraissent avoir fort justement désigné son ou-

---

([1]) Cette nécessité avait déjà été comprise par plusieurs de nos Maîtres, et tout particulièrement par celui dont la perte vient de nous éprouver tous cruellement.

vrage à l'attention de M. Lévy pour la publication qu'il nous présente aujourd'hui et dont j'ai essayé, dans ce qui précède, de faire comprendre l'importance scientifique.

Je ne doute donc pas, pour ma part, que ceux qui, dans notre pays tiennent à suivre les progrès des mathématiques, ne saisissent l'occasion qui leur est offerte de s'initier, par l'étude des cas les plus simples, à une doctrine profonde et difficile, et que, par conséquent, l'ouvrage actuel ne rencontre tout le succès que je lui souhaite.

J. Hadamard.

1er Novembre 1910.

PRÉFACE DE L'AUTEUR

Depuis que Gauss a élargi le champ de l'arithmétique en y introduisant les nombres de la forme $a + b\sqrt{-1}$ il s'est formé une théorie splendide de nombres algébriques. Les noms de Kummer, de Dirichlet [1], Dedekind et Kronecker et ceux de quelques mathématiciens célèbres de notre époque se rattachent à l'histoire de son développement. Cette théorie a souvent modifié son aspect extérieur et nous possédons des ouvrages d'ensemble signés de noms très autorisés, Dedekind, Hilbert [2], Kronecker [3] et Hensel ainsi que celui qui a été publié récemment par M. Bachmann [4], qui exposent les résultats sous différents points de vue.

Tous ces livres comprennent le cas le plus général de la théorie et sont difficiles à lire pour un débutant. Aussi j'ai pensé qu'il serait utile d'en faire une exposition qui permît de faire connaître de la façon la plus élémentaire possible, les problèmes et les résultats de cette théorie.

---

[1] P.-G. Lejeune-Dirichlet et Dedekind. *Vorlesungen über Zahlentheorie*, 4e édit *Braunschweig*, 1894. Suppl. XI.

[2] D. Hilbert. *Die Theorie der algebraischen Zahlkörper. Bericht, erstattet der deutschen Mathematiker-Vereinigung. Jahresbericht der deutschen Math.-Vereinigung*, t. IV. Berlin, 1894

Cet ouvrage sera cité dans cet ouvrage sous le nom de *Zahlber*, ou *Bericht*.

[4] L. Kronecker. *Vorlesungen über Zahlentheorie*, édité par K. Hensel, Berlin 1901.

[4] P. Bachmann. *Zahlentheorie*, t. V; *Allgemeine Arithmetik der Zahlkörper*, Leipzig, 1905.

Il faudrait citer ici aussi plusieurs chapitres de H. Minkowski. *Geometrie der Zahlen*, Leipzig, 1896-1910.

J'ai pensé atteindre ce but en traitant particulièrement le cas des corps les plus simples, le corps quadratique et le corps cubique.

La lecture de ce livre ne nécessite que peu de connaissances tirées de l'algèbre. J'ai tâché d'atteindre toujours mon but par les méthodes les plus simples, et je me suis rapproché des travaux sur cette théorie qui m'ont paru les plus clairs et que l'on trouve dans les œuvres de MM. Hurwitz, Hilbert et Minkowski. J'ai utilisé aussi le cours fait pendant l'hiver 1897-1898 dans lequel M. Hilbert nous a exposé entre autres choses : l'étude du corps quadratique et ses applications au « dernier théorème de Fermat ». J'ai toujours pris pour modèle son exposition claire et irréprochable.

M. le Dr. A. Timpe à Danzig et M. le Privatdozent Dr. R. Fueter à Marbourg m'ont prêté leur concours pour la correction des épreuves. Grâce aux précieux conseils de ce dernier, j'ai pu améliorer bien des détails de certaines démonstrations. Je leur exprime ma reconnaissance. Mais je dois beaucoup à M. le conseiller intime Hilbert qui m'a encouragé dans mon travail, ses conversations m'ont été d'un secours précieux. Il a de plus mis à ma disposition avec une attention amicale le manuscrit d'un cours fait par lui antérieurement et qui m'a servi pour un point essentiel (n° 15).

Langfuhr, décembre 1906.

J. SOMMER.

NOTE DU TRADUCTEUR

J'ai employé les expressions de forme ambige, idéal ambige — au lieu de forme ambiguë, idéal ambigu. — Le mot ambigu a dans la langue française un sens qu'on ne saurait lui retrouver ici.

A. LÉVY.

INTRODUCTION A LA THÉORIE
DES NOMBRES ALGÉBRIQUES

CHAPITRE PREMIER

—

INTRODUCTION

Nous allons exposer tout d'abord la théorie du corps quadratique, dans le but d'étendre les théorèmes acquis pour les nombres naturels à des nombres ayant plus de généralité.

Cette généralisation n'est pas seulement intéressante en elle-même, mais elle nous permettra de déduire simplement des faits de la théorie des nombres « rationnels » comme conséquences de la théorie générale, alors que ces faits seraient très difficiles à établir avec nos ressources actuelles.

Nous commencerons par rappeler d'une manière un peu concise les théorèmes les plus importants de la théorie élémentaire que nous devrons retrouver dans la théorie générale (1).

(1) Pour toute étude particulière l'auteur renvoie aux excellents ouvrages :

P.-G. Lejeune-Dirichlet. — *Vorles. uber Zahlentheorie, Herausgeg. von Dedekind* 4. Aufl. 1894.

Ph. Tschebyscheff. — *Théorie des Congruences*, éd. allem. de Schapira. Berlin 1889.

P. Bachmann. — *Théorie des Nombres*, t. I. Eléments. Leipzig 1872.

P. Bachmann. — *Niedere Zahlentheorie*, 1e partie, 1902.

H.-S. St-Smith. — *Collected mathematical papers*, vol. I. *Report on the theory of nombers*, 6 parts, p. 38-364, 1894, Oxford 1894. Les six parties du rapport ont paru d'abord de 1859 à 1865 dans les *Reports of the British Association*, œuvres originales de Lagrange, Gauss, Legendre, Dirichlet.

C.-F. Gauss. — *Disquisitiones arithmeticae* Leipz. 1801. Œuvres complètes t. I, et trad. française, Paris, Hermann, 1910.

A.-M. Legendre. — *Théorie des Nombres*, 4e éd. Paris, 1900, 2 volumes.

1. Divisibilité des entiers rationnels. — Nous désignerons les nombres entiers positifs et négatifs par les lettres françaises a, b, c ... en particulier les nombres quelconques par a, b, c ... les nombres premiers par p, q.

Un nombre est premier lorsqu'à part lui-même il n'admet d'autres diviseurs que ± 1. a et b sont premiers entre eux lorsqu'il n'y a pas de nombre premier p, q qui les divise tous les deux.

Le *théorème fondamental* de la théorie des nombres rationnels dit que tout nombre entier ne peut être décomposé essentiellement que d'une seule manière en facteurs premiers. Nous ajoutons le mot « essentiel » pour dire que nous ne distinguerons point les facteurs positifs et négatifs.

La démonstration de ce théorème s'appuie sur la méthode suivie par Euclide pour trouver le plus grand commun diviseur de deux nombres. Rappelons-là : soient a et b deux nombres (supposons-les positifs pour plus de simplicité). Si $a > b$ on peut poser

$$a = b \times q + r_0 \qquad 0 \leqq r_0 < b \text{ (}^1\text{)}$$

si $r_0 > 1$ on divise b par r_0 et on a

$$b = q_1 r_0 + r_1 \qquad 0 \leqslant r_1 < r_0$$

et ainsi de suite, on obtient un nombre fini d'opérations

$$\cdots\cdots\cdots$$

$$r_{n-2} = q_n r_{n-1} + r_n$$

et on aura $r_n = 1$ ou $r_n = 0$ après $n + 1$ opérations, d'ailleurs $n + 1 < b$.

Si $r_n = 1$, a et b sont premiers entre eux.

Si $r_n = 0$ r_{n-1} est le plus grand commun diviseur de a et de b. et tout diviseur commun à a et à b divise r_{n-1}.

On en déduit que

Lemme. Si b divise le produit aa_1, et s'il est premier avec a il divise a_1.

---

(1) Note du traducteur. — Cette démonstration étant enseignée dans toutes les écoles françaises, je me suis permis d'abréger ici un peu le texte de M. Sommer.

En effet si a et b sont premiers entre eux, leur plus grand commun diviseur est 1, celui de aa_1 et ba_1 est a_1 or b divisant aa_1 et ba_1 divise a_1.

Réciproquement si le nombre premier p est premier avec a et avec a_1 il ne peut diviser aa_1.

On arrive alors au résultat suivant :

Théorème fondamental. — Un nombre entier positif a ne peut être décomposé que d'une seule manière en un produit de facteurs premiers positifs.

Démonstration : Admettons que l'on ait à la fois

$$a = p_1 \cdot p_2 \cdot p_3 \cdots p_\nu$$

$$a = q_1 q_2 \cdots q_\mu$$

ou $p_1 p_2 \ldots p_\nu$ ainsi que $q_1 \ldots q_\mu$ désignent les nombres premiers distincts entre eux ou non, a, c'est-à-dire le produit $p_1 p_2 \ldots p_\nu$ est divisible par q_μ ce qui serait impossible si tous les p étaient différents de q_μ, nous pouvons donc admettre que $p_\nu = q_\mu$ et nous verrons de même que $p_{\nu-1} = q_{\mu-1}$, etc. Enfin $\nu = \mu$ et $p_1 = q_1$ $p_2 = q_2 \ldots$

D'ailleurs le théorème fondamental est vrai d'une façon générale pour des nombres et des facteurs positifs ou négatifs, lorsque deux de ces décompositions sont considérées comme essentiellement égales quand les facteurs ne diffèrent que par le signe.

2. La fonction $\varphi(m)$. — ***Problème.*** Soit m un entier positif, trouver le nombre des entiers de la suite 1, 2 ... $m - 1$ premiers avec m.

Solution : Soit $\varphi(m)$ [1] le nombre cherché. Si m ne contient qu'un diviseur premier p $m = p$

$$\varphi(p) = p - 1 = p\left(1 - \frac{1}{p}\right). \tag{1}$$

---

(1) Symbole dû à Gauss pour désigner ce nombre déjà trouvé par Euler. *Disquisitiones arithmeticae*, sect. II, art. 38.

Soit $m = p^k$ les seuls nombres inférieurs à m et non premiers avec lui sont

$$p,\ 2p,\ 3p,\ \ldots\ (p^{k-1} - 1)\,p$$

donc

$$(2) \qquad \varphi(p^k) = p^k - 1 - (p^{k-1} - 1) = p^k\left(1 - \frac{1}{p}\right).$$

Soit $m = p_1^{k_1}\,p_2^{k_2} \ldots p_1^{k_n}$ et supposons connu $\varphi(m)$, voyons si nous saurons déterminer $\varphi(m_1)$

$$m_1 = p_1^{k_1}\,p_2^{k_2} \cdots p_n^{k_n}\,p_{n+1}^{k_{n+1}}.$$

D'après notre hypothèse il y a

$$(3) \qquad \Psi(m_1) = p_{n+1}^{k_{n+1}}\,\varphi(m)$$

nombres inférieurs à m_1 et premiers avec m, car dans chaque intervalle 1 à m, m à $2m$, ... et ainsi de suite jusqu'à $\left(p_{n+1}^{k_{n+1}} - 1\right)m$ à $p_{n+1}^{k_{n+1}}m$ il y a $\varphi(m)$ nombres répondant à la question. Mais parmi ces nombres il y a encore ceux qui contiennent une ou plusieurs fois le facteur p_{n+1} et qui sont premiers avec m, c'est-à-dire qui ne contiennent aucun des facteurs $p_1\,p_2 \ldots p_n$. Dans la suite

$$1\,p_{n+1},\ 2\,p_{n+1},\ \cdots\ \frac{m_1}{p_{n+1}} \times p_{n+1}$$

il faut prendre les facteurs $1\,p \ldots \frac{m_1}{p_{n+1}}$ qui sont premiers avec m, on obtient une expression analogue à (3)

$$p_{n+1}^{k_{n+1}-1}\,\varphi(m)$$

$$\varphi(m_1) = p_{n+1}^{k_{n+1}}\,\varphi(m) - p_{n+1}^{k_{n+1}-1}\,\varphi(m) = \varphi(m)\,p_{n+1}^{k_{n+1}}\left(1 - \frac{1}{p_{n+1}}\right).$$

Nous avons maintenant une formule de récurrence qui donne

$$(4) \qquad \varphi(m) = m\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_n}\right)$$

d'où résulte le théorème

$$\varphi(m) = \varphi(m_1)\,\varphi(m_2)$$

faisons de plus $\varphi(1) = 1$ et nous aurons :

Théorème. — Soit m un nombre quelconque et si l'on remplace t successivement par tous les diviseurs de m on a $\sum_t \varphi(t) = m$.

Démonstration : Soit

$$m = a = p^k$$

les diviseurs de a sont $1, p, p^2 \ldots p^k$

$$\sum(t_a) = \varphi(1) + \varphi(p) + \varphi(p^2) + \ldots \varphi(p^k) = p^k = a$$

Soit en général

$$m = p_1^{k_1} \cdot p_2^{k_2} \ldots p_n^{kn} = a_1, a_2 \ldots a_n$$

les diviseurs de m sont les nombres du produit

$$\left(1 + p + \ldots p_1^{k_1}\right)\left(1 + p_2 + \ldots + p_2^{k_2}\right) \ldots \left(1 + p_n + \ldots + p_n^{kn}\right)$$

appliquons le théorème précédent à chaque diviseur, nous aurons

$$\left[\left(\varphi(1)+\varphi(p)\right)+\ldots\varphi\left(p_1^{k_1}\right)\right]\left[\varphi(1)+\varphi(p_1)+\ldots\varphi\left(p_2^{k_2}\right)\right]$$
$$= \sum\varphi\left(t_{a_1}\right) + \sum\varphi\left(t_{a_2}\right) \ldots \sum\varphi\left(t_{a_n}\right)$$
$$= a_1, a_2 \ldots a_n = m.$$

Ce théorème joue un rôle important lorsqu'on veut démontrer l'existence de racines primitives.

3. Les congruences. — Gauss [1] emploie la notation $a \equiv 0$ (mod. m) ou encore $a \equiv 0\ (m)$ pour indiquer que a est divisible par m. On dit que a est congru à o suivant le module m. Dire que $a - b \equiv 0\ (m)$ ou que $a \equiv b\ (m)$, ou dire a est congru à b sui-

---

[1] Gauss. — *Disquis. arithm.* Sect. I. Art. (1), (3).

vant le module m, c'est exprimer que la différence $a - b$ est divisible par m.

De cette définition résultent :

I. Si $a \equiv b\ (m)$, $a \equiv c\ (m)$, on a aussi $b \equiv c\ (m)$.

II. Si $a \equiv b\ (m)$, $c \equiv d\ (m)$, $a + c \equiv b + d\ (m)$, et aussi $ac \equiv bd\ (m)$.

III. Si n est un entier rationnel premier avec m, $a \equiv b\ (m)$, donne $an \equiv bn\ (m)$.

Et aussi de

$$an \equiv bn\ (m)$$
$$a \equiv b\ (m) \quad \text{lorsque} \quad n \not\equiv 0\ (m).$$

La représentation symbolique des congruences d'après Gauss, est très commode et très fertile, elle a pris le droit de cité.

Cette façon d'écrire

$$a \equiv b\ (m)$$

montre bien que la divisibilité d'un nombre par un autre dans certaines questions entre seule en jeu et que la valeur du quotient n'a pas d'importance.

On a réparti tous les nombres ou *classes* suivant le module m, deux nombres a et b étant considérés comme équivalents, suivant le module m, s'ils sont congrus suivant le module m, c'est-à-dire si divisés par m, ils donnent le même reste.

Les nombres se répartissent en m classes, suivant le module m, tout nombre étant congru à un nombre de la suite

$$0, 1, 2 \ldots m - 1$$

et à un seul ; tandis que deux nombres de cette suite ne peuvent être congrus entre eux. Si m est impair, les m entiers compris entre $-\frac{m-1}{2}$ et $+\frac{m-1}{2}$ et dans le cas où m est pair, les entiers compris entre $-\frac{m}{2} + 1$ et $\frac{m}{2}$ forment le système des restes les plus petits en valeur absolue suivant le module m, ou encore la série des restes absolus.

4. Le théorème de Fermat. *Théorème* (¹). — Soit p un nombre premier rationnel, a un nombre entier qui n'est pas divisible par p, on a :

$$a^{p-1} - 1 \equiv 1 \ (p)$$

Démonstration : Considérons la suite de $p - 1$ nombres

$$a, 2a, 3a \dots (p-1)a$$

deux nombres de cette suite ka et ha ne peuvent être congrus à a, car p ne peut diviser $(k-h)a$, il est premier avec a, et comme $k \leqq p - 1$, $h \leqq p - 1$, p ne peut diviser $k - h$, les restes des nombres de cette suite par p, sont donc dans un certain ordre, $1, 2, \dots p - 1$. Si on désigne ces restes par $r_1 r_2 \dots r_{p-1}$, on a

(2) $$1 . 2 \dots (p-1) a^{p-1} \equiv r_1 . r_2 \dots r_{p-1}, \ (p)$$

et par suite

$$1 . 2 \dots (p-1) a^{p-1} \equiv 1 . 2 \dots (p-1) \ (p)$$

c'est-à-dire

$$a^{p-1} \equiv 1 \ (p).$$

On a quel que soit a

$$a^p \equiv a \ (p)$$

Euler a montré que l'on a de plus

$$a^{\varphi(m)} \equiv 1 \ (m)$$

si a est premier avec m. La démonstration est en tout point semblable à la précédente.

Nous ferons de ce théorème, les applications suivantes :

Problème. — Soit $ax \equiv b \ (m)$, où $a \not\equiv o$, b, $m \not\equiv o$ sont donnés, cherchons les valeurs de x qui satisfont à cette congruence.

(¹) C'est à ce théorème que l'on donne le nom de théorème de Fermat. Il a été démontré par Euler et par Lagrange. Fermat a énoncé sans démonstration le théorème que nous indiquons plus loin relatif à $a^t \equiv 1 \ (p)$, dans une lettre à Frénicle du 18 octobre 1640. Voir œuvres de Fermat publ. par P. Tannery et Ch. Henry, tome II, Paris 1894, p. 209.

Solution 1. Supposons d'abord a et m premier entre eux, alors $a^{\varphi(m)} \equiv 1$. Multipliant les deux nombres de la congruence

$$ax \equiv b\ (m) \quad \text{par} \quad a^{\varphi(m)-1}$$

il vient

$$x \equiv b\ .\ a^{\varphi(m)-1}\ (m)$$

on a donc une solution.

Soient x_1, x_2 deux solutions distinctes

$$ax_1 \equiv b\ (m)$$
$$ax_2 \equiv b\ (m)$$

nous donnent $x_1 - x_2 \equiv 0\ (m)$, la solution générale est donc

$$x \equiv b\ .\ a^{\varphi(m)-1} + m\ .\ s.$$

2. a et m ne sont pas premiers entre eux. Soit t leur plus grand commun diviseur, alors

$$ax \equiv b\ (m)$$

que l'on peut écrire sous la forme

$$ax - my = b$$

nous montre qu'il y a une condition de possibilité, il faut que t divise b. Si elle est remplie en divisant par t, on ramène à la forme

$$a_1 x \equiv b_1\ (m_1)$$

où a_1 est premier avec m_1

Si on désigne par x_1 la valeur

$$x_1 = b_1 a_1^{\varphi(m_1)-1}$$

les solutions sont données par

$$x_1 + m_1 s$$

nous considérerons le système des valeurs incongrues, suivant m

$$x_1,\ x_1 + m \quad x_1 + 2m \ldots x_1 + (t-1)\ m$$

qui nous donnent les t racines incongrues suivant m de la congruence. On peut exprimer ce qui précède sous la forme :

Théorème. — L'équation indéterminée

$$ax - my = b$$

à coefficients entiers rationnels a, b, m n'a des solutions que si le plus grand commun diviseur t de a et de m divise b.

Les solutions c'est-à-dire les valeurs numériques de x et y en nombre infini peuvent être représentées par t valeurs incongrues suivant le module m.

D'après cela si t est le plus grand diviseur de a et de b, on peut toujours trouver deux entiers x et y tels que $ax + by = t$. Ce théorème va nous permettre une seconde application du théorème de Fermat.

Théorème. — Soit p un nombre premier positif et rationnel et a un entier qui n'est pas divisible par p, le plus petit exposant e pour lequel

$$a^e \equiv 1\ (p)$$

est un diviseur de $p - 1$.

Il est tout d'abord évident que $e > 1$, sauf le cas $a = 1$ ou $a \equiv 1\ (p)$. D'abord toutes les puissances a^1, a^2, a^3 ... a^{e-1} sont incongrues (p), car si ou avait $a^{e_1} \equiv a^{e_2}$ module p, $e_2 < e_1 < e$, il en résulterait

$$a^{e_2}\left(a^{e_1 - e_2} - 1\right) \equiv 0\ (p)$$

c'est-à-dire

$$a^{e_2 - e_1} \equiv 0\ (p).$$

ce qui est contraire à l'hypothèse.

Supposons que e ne divise pas $p - 1$ on pourrait trouver deux entiers x et y tels que $ex + (p-1)y = e'$ e' étant le plus grand commun diviseur de e et de $p - 1$. De $a^e \equiv 1$ $a^{p-1} \equiv 1\ (p)$ il résulte que $a^{ex}a^{(p-1)y} \equiv 1$ c'est-à-dire $a^{e'} \equiv 1\ (p)$ e' étant $< e$. Il faut donc que e divise $p - 1$.

On dit alors que a appartient à l'exposant e.

Les nombres w qui appartiennent à l'exposant $p - 1$ ont une

signification particulière. Euler les nomme *racines primitives* suivant p. Les puissances successives

$$w\ w^2\ w^3\ \ldots\ w^{p-1}$$

donnent pour reste par p dans un certain ordre les nombres

$$1\ 2\ 3\ \ldots\ (p-1).$$

Gauss (¹) a démontré par un raisonnement célèbre l'existence de ces racines, — nous le donnerons au sujet des nombres quadratiques. Voici d'ailleurs l'énoncé du théorème.

Théorème. — Il y a $\varphi(e)$ nombres incongrus suivant le module p appartenant à l'exposant e, e étant un diviseur de $p-1$, en particulier il y a toujours $\varphi(p-1)$ nombres appartenant à l'exposant $(p-1)$.

Exemple : $p = 7$ e divise $p - 1 = 6$.

$1 : \varphi(1) = 1$	1 nombre	$a = 1$
$2 : \varphi(2) = 1$	1 nombre	$a = 6$
$3 : \varphi(3) = 2$	2 nombres	$a = 2, 4$
$4 : \varphi(6) = 2$	» »	$a = 3, 5.$

Congruences entières de degré supérieur.

On appelle ainsi des congruences de la forme

$$a_0x^n + a_1x^{n-1} + \ldots a_n \equiv 0\ (a)$$

où x désigne une inconnue, et où $a_0 \ldots a_n$ sont des coefficients rationnels entiers. Si $a_0 \not\equiv 0\ (a)$ une telle congruence est dite de degré n, x, est dit une racine de cette congruence si x rend le premier membre divisible par a.

Théorème. — Si $f(x) = a_0x^n + a_1x^{n-1} + a_n \equiv 0\ (p)$ a une racine p étant un nombre premier il existe toujours une racine x, telle que $f(x) \equiv 0\ (p)$ mais que $f(x) \not\equiv 0\ (p^2)$ — car si $x = a$ satisfait à $f(a) \equiv 0\ (p^2)$ on peut déterminer l entier de telle sorte que $x_1 = a + lp$ satisfasse à la condition de l'énoncé.

De même qu'on démontre en algèbre qu'une équation de degré n $f(x) = 0$, a n racines on démontre que :

(¹) *Disqu. arithm.* III 52 à 55.

Théorème. — Une congruence de degré n suivant un module premier p

$$f(x) = a_0 x^n + a_1 x^{n-1} + \dots + a_n \equiv 0 \ (p)$$

a au plus n racines distinctes suivant le module p.

On a $f(x) = (x - \alpha) f_1 x + f(\alpha)$ si α est racine de la congruence $f(\alpha) \equiv 0$ mod. p et toute racine de $f_1(x) \equiv 0$ est une racine de $f(x) \equiv 0$ $f(x)$ ne peut donc avoir en plus des racines de la seconde que la racine $x = \alpha$ c'est-à-dire une racine de plus que la seconde. Or la congruence du premier degré n'a qu'une racine, celle du second en a au plus deux, celle du troisième au plus 3, etc.

Ceci ne veut pas dire que la congruence a n racines, elle peut en avoir moins, ou ne pas en avoir du tout. Il faudra examiner chaque congruence en particulier pour savoir si elle admet des racines. La plus simple est $n = 2$. Une congruence du second degré suivant un module premier p peut toujours être ramenée à la forme

$$x^2 - m \equiv 0 \ (p).$$

Lorsque cette congruence admet la racine w, elle admet aussi la racine $-w$. Si m est premier avec p on dit alors que m est reste quadratique de p, dans le cas où la congruence n'a pas de racines on dit que m est non-reste. Legendre introduit le symbole suivant $p > 2$.

$$\left(\frac{m}{p}\right) = +1 \text{ quand } m \text{ reste quadratique de } p$$

$$\left(\frac{m}{p}\right) = -1 \text{ quand } m \text{ est non-resté quadratique de } p.$$

Ce symbole avec les conditions énoncées plus haut est donc toujours égal à $+1$ ou à -1. Nous apprendrons à le calculer plus loin au nº 26.

Ce qui précède nous permet cependant d'établir quelques propriétés du symbole. Désignons par w une racine primitive du nombre premier impair p, alors par une certaine valeur de l'exposant M on a

$$m \equiv w^M \ (p)$$

La congruence

$$x^2 - w^M \equiv 0 \ (p)$$

n'admet de solution que si M est un nombre pair, la condition est suffisante. D'où un théorème dû à Euler :

Théorème. — m est reste quadratique de p ou non-reste suivant que

$$m^{\frac{p-1}{2}} \equiv +1\,(p) \quad \text{ou} \quad m^{\frac{p-1}{2}} \equiv (-1)\,p$$

ou encore on a toujours

$$\left(\frac{m}{p}\right) \equiv m^{\frac{p-1}{2}}\,(p).$$

Soient m et m_1, deux nombres entiers quelconques, dont aucun n'est divisible par p et si l'on pose

$$m = w^{M}\,(p) \qquad m_1 = w^{M_1}\,(p)$$
$$mm_1 = w^{M+M_1}\,(p)$$
$$\left(\frac{mm_1}{p}\right) = (mm_1)^{\frac{p-1}{2}}\,(p)$$

ou

$$\left(\frac{m}{p}\right)\left(\frac{m_1}{p}\right) = \left(\frac{mm_1}{p}\right).$$

Cette dernière égalité nous donne la règle de la multiplication qui permet de ramener le calcul de ce symbole $\frac{q}{p}$ au cas où q et p sont premiers. En particulier si m est négatif

$$\left(\frac{-m}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{+m}{p}\right).$$

Je m'arrêterai là dans l'énumération des faits de la théorie élémentairedes nombres rationnels je veux passer aux recherches relatives aux nombres algébriques, j'aurais alors l'occasion de revenir sur les questions que je viens d'indiquer.

La théorie des nombres algébriques est une branche relativement nouvelle de la théorie des nombres. C'est Gauss qui en a été l'initiateur. Euler puis Legendre et Gauss avaient vu indépendamment l'un de l'autre la réciprocité des solutions de

$$x^2 - q \equiv 0\,(p) \qquad \text{et} \qquad x^2 - p \equiv 0\,(q)$$

p. q. étant premiers. Cette réciprocité merveilleuse s'exprime par le symbole

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

Gauss parvint à démontrer le premier d'une manière irréprochable cette loi de réciprocité, il en a donné six démonstrations fondées sur des principes tout à fait différents. Mais lorsque Gauss (1) voulut étendre ce théorème fondamental à des congruences de degrés supérieure, et qu'en particulier il étudia $x^4 - q \equiv 0\ (p)$ il trouva bien toute une suite de théorèmes particuliers, mais le théorème général de réciprocité « biquadratique » lui échappa tant qu'il se maintint dans le domaine des nombres réels rationnels, et les démonstrations suffisantes pour des cas particuliers ne valaient plus pour la généralité des nombres rationnels. Les difficultés (2) disparurent lorsque Gauss inventa « une extension originale du domaine de l'arithmétique supérieur » et lorsqu'il donna aux nombres complexes $a + b\sqrt{-1}$ « exactement les mêmes droits de cité » qu'aux entiers rationnels (3).

Ce fait a porté ses fruits. Gauss avec l'heureuse intuition du génie a ouvert de nouveaux et riches domaines à la science.

Bientôt on vit que le théorème de réciprocité cubique s'expose le plus facilement en partant des nombres $a + b\,\frac{1 + \sqrt{-3}}{2}$ et on obtint des résultats analogues pour les théorèmes de réciprocité plus élevés. La solubilité de $x^n + y^n = z^n$ exigeait d'elle-même la considération de nombres complexes, formées de racines $n^{\text{èmes}}$ de l'unité, et aussi dans le domaine des fonctions elliptiques, la multiplication complexe montra la nécessité d'introduire des nombres de la forme $a + b\sqrt{m}$.

Ce qui fait la valeur principale de l'étude des corps dans la théorie des nombres, consiste en ce qu'elle l'a enrichie de méthodes bien plus générales. On s'en rendra probablement compte dans cer

---

(1) C. F. GAUSS — *Théoria residuorum biquadraticorum*. Ges. W. t. II p. 67 *und Besprech* p. 165.

(2) C. F. GAUSS. — *Werke*, t. II, p. 95 et 169.

(3) C. F. GAUSS. — *Werke*, t. II, p. 171.

tains chapitres de ce livre. De plus en plus à la suite des découvertes (provoquées par Gauss) faites par des arithméticiens du siècle dernier, la théorie des nombres supporte la comparaison avec l'analyse générale en ce qui concerne l'étendue et la richesse des méthodes. De sorte qu'elle ne sera bientôt plus la propriété exclusive de quelques rares esprits privilégiés.

L'arithmétique des nombres complexes

$$a + b\sqrt{-1} \qquad a + b\frac{1 + \sqrt{-3}}{2}$$

n'exige pas de nouveaux principes par rapport à la théorie élémentaire des nombres réels. On peut l'exposer comme une généralisation de la première, elle a été représentée de bien des manières [1]. Pour ne pas importuner par des répétitions, nous énoncerons ici comme entrée en matière les principaux résultats. Les démonstrations sont contenues dans la suite.

Un nombre complexe $a + b\sqrt{-1}$ est un « entier » lorsque a et b sont des entiers rationnels. La somme, la différence, le produit de deux entiers complexes est encore un nombre complexe entier. De plus, soient $\alpha\ \beta\ \gamma$ trois nombres complexes et soit $\alpha = \beta \cdot \gamma$, on dit que α est divisible par β et par γ, ou encore β est contenu dans α. Il y a outre ± 1 les nombres entiers $\pm\sqrt{-1}$ qui divisent 1 et les quatre nombres $\pm 1 \pm \sqrt{-1}$ sont dits les unités du corps.

Comme on peut démontrer (voir p. 27) que l'algorithme d'Euclide s'applique à deux nombres quelconques α et β on peut généraliser la notion de nombre premier, et on a le théorème : Tout nombre complexe ne peut être décomposé d'une manière essentielle en facteurs premiers, si l'on ne tient pas compte des facteurs unités.

Tout nombre complexe premier divise un nombre premier réel,

$$2 = (1 + \sqrt{-1})(1 - \sqrt{-1})$$

de plus tout nombre premier $p \equiv 1\ (4)$ se décompose en deux nombres premiers distincts

$$\pi = x + y\sqrt{-1} \qquad \pi' = x - y\sqrt{-1}$$

---

[1] C.-F. Gauss. — *Dirichlet-Dedekind*, *Vorlesungen*, suppl. XI, p. 435.

par contre tout nombre entier premier $p \equiv 3\ (4)$ est aussi premier dans le domaine des nombres complexes.

Tout nombre entier complexe $a + b\sqrt{-1}$ peut être pris pour module d'une congruence linéaire, quadratique ou autre, l'étude de ces congruences se généralise facilement dans le nouveau domaine.

A tout nombre $a + b\sqrt{-1} = \alpha$ correspond un système de $\alpha^2 + b^2$ nombres tel que deux d'entre eux soient incongrus suivant le module α, tandis que tout nombre réel ou complexe est congru à l'un des nombres du système suivant le module α.

Le théorème de Fermat pour les nombres complexes s'énonce : Soit $\pi = x + y\sqrt{-1}$ un nombre premier complexe et α un entier qui n'est pas divisible par π on a toujours

$$\alpha^{x^2+y^2-1} \equiv 1\ (\pi)$$

et on rattache à ce théorème la notion de racine primitive ainsi que l'étude des congruences quadratiques et de la loi de réciprocité.

CHAPITRE II

—

LE CORPS QUADRATIQUE

5. Définitions. — Le mot *corps de nombre*, ou *domaine de nombres* ou *domaine* est emprunté à la nomenclature de la théorie générale des nombres, ou plutôt de l'algèbre. Il a été introduit dans la science par Dedekind et par Kronecker. Il représente un système infini de grandeurs, permettant sans réserve les opérations fondamentales : addition, soustraction, multiplication, division. Le résultat de toutes ces opérations sauf la division par o faites sur des grandeurs quelconques du système donne encore une grandeur du système.

On dit par exemple, que l'ensemble des nombres rationnels forme un corps ou qu'il appartient à un domaine. Soient $ab \ldots x$ des nombres rationnels, on a l'habitude de dire que l'équation

$$ax + b = 0 \qquad \text{ou} \qquad a + x = b$$

est toujours résoluble dans le domaine des nombres rationnels, à moins que dans le premier exemple on ait $a = 0$.

Par contre toute équation quadratique

$$ax^2 + b = 0 \qquad \text{ou} \qquad ax^2 + bx + c = 0$$

dont les coefficients appartiennent au domaine des nombres rationnels n'est pas toujours résoluble dans le domaine précédent. Ces équations deviennent solubles si l'on adjoint au corps des nombres rationnels une expression de la forme $\sqrt{m}$ où m est un nombre entier rationnel.

On étend la notion de nombre, en appelant nombre toute

expression de la forme $u + v\sqrt{m}$, u v désignant des nombres rationnels. Pour les distinguer des nombres naturels nous dirons que les nombres $u + v\sqrt{m}$ sont des *nombres algébriques*. Tout nombre de cette forme satisfait à une équation du second degré $ax^2 + bx + c = 0$ à coefficients entiers, c'est pourquoi les expressions de la forme $u + v\sqrt{m}$ sont dits des *nombres quadratiques*.

Soit m un nombre rationnel quelconque et soit $\sqrt{m}$ la racine positive de $x^2 - m = 0$, adjoignons cette grandeur $\sqrt{m}$ au domaine des entiers et effectuons les quatre opérations élémentaires dans ce nouveau domaine de toutes les façons possibles. Nous obtiendrons toutes les fonctions rationnelles de $\sqrt{m}$. Mais comme

$$(\sqrt{m})^2 = m \qquad (\sqrt{m})^3 = m\sqrt{m} \text{ etc.}$$

toutes les expressions obtenues seront de la forme

$$\frac{a + b\sqrt{m}}{a_1 + b_1\sqrt{m}}$$

ou plus simplement de la forme

$$\frac{a + b\sqrt{m}}{c}$$

où a b c a_1 b_1 sont des nombres entiers rationnels ou 0, le cas ou a_1 et b_1 seuls ou bien ou c seul égalent 0 étant excepté.

Dans le sens que nous avons dit plus haut, ces fonctions rationnelles forment un *domaine de rationnalité* (1) ou *un corps de nombres* (2), ou plus brièvement un *corps* (Dedekind), car la somme, la différence, le produit, le quotient de deux pareilles fonctions est encore de la même forme.

Nous désignerons le corps particulier que nous venons de définir par *corps quadratique*. Il est parfaitement déterminé par le nombre $\sqrt{m}$, c'est pourquoi nous écrirons $k(\sqrt{m})$.

---

(1) L. Kronecker. — *Grundzüge einer arithmet. Theorie der algebr. Grössen* 1882. W. Bd. II, p. 148.

(2) Dirichlet. — *Vorlesungen*, 4. Aufl. Suppl. XI, p. 452. Pour les démonstrations, comparer Hilbert Zahlb, chap. I, III et XVI.

Lorsqu'il n'y aura pas de confusion à craindre, on écrira « *le corps k* ».

Il est évident que le corps des nombres rationnels est un corps quadratique particulier, et que tout corps $k(\sqrt{m})$ contient entièrement le corps des nombres rationnels. On dit qu'on obtient le corps $k\sqrt{m}$ en adjoignant au corps des nombres rationnels la grandeur $\sqrt{m}$.

Tout d'abord les deux propositions suivantes sont évidentes.

1. Le corps $k(-\sqrt{m})$ est identique au corps $(k\sqrt{m})$.

2. Si δ est une racine de l'équation

$$a_0x^2 + 2a_1x + a_2 = 0 \quad \text{et} \quad m = a_1^2 - a_0a_2$$

le corps $k(\delta)$ est identique au corps $k\sqrt{m}$ et les deux racines δ_1, δ_2 définissent le même corps.

Qu'est ce qui correspond à la notion de nombre entier rationnel, et de nombre fractionnaire rationnel dans le corps quadratique. Il sera bon de généraliser la notion « de nombre entier » de telle sorte que la notion généralisée conserve son sens dans le cas particulier des nombres rationnels, c'est-à-dire que tout nombre entier du corps quadratique qui est rationnel soit un entier rationnel. Il faudra avant tout exiger pour la notion de nombre « entier » que les nombres entiers du corps quadratique soient invariants pour les mêmes opérations que dans le domaine des nombres rationnels ; c'est-à-dire que des nombres entiers soumis à ces opérations donnent encore des nombres entiers.

La somme, la différence, le produit de deux entiers est un entier et l'on désire qu'il en soit de même dans le corps quadratique. De plus chaque nombre doit apparaître sous sa forme la plus simple et n'avoir qu'une représentation unique, c'est-à-dire que si on le prend sous la forme

$$\frac{a + b\sqrt{m}}{c}$$

le numérateur et le dénominateur ne doivent avoir aucun facteur commun.

La définition suivante répond aux conditions indiquées :

Définition. — Un nombre d'un corps quadratique est dit entier lorsqu'il satisfait à une équation du second degré de la forme

$$x^2 + a_1x + a_2 = 0$$

où le coefficient de x^2 est 1 et les coefficients a_1 et a_2 sont des entiers rationnels.

De cette définition nous déduirons immédiatement le :

Théorème. — Tout entier d'un corps quadratique qui est rationnel est un nombre entier rationnel.

Démonstration : Soit α un entier du corps satisfaisant à

$$x^2 + a_1 x + a_2 = 0.$$

Soit α un nombre rationnel on peut le mettre sous la forme $\alpha = \frac{a}{b}$ ou a et b sont des entiers premiers entre eux. On aurait donc

$$\frac{a^2}{b^2} + a_1 \frac{a}{b} + a_2 = 0$$

$$\frac{a^2}{b} = -(a_1 a + a_2 b).$$

Comme le nombre du second membre est entier $\frac{a^2}{b}$ doit être entier, c'est-à-dire $b = 1$ et $\alpha = a$ un nombre entier rationnel.

Notation. — Nous désignerons dorénavant les nombres (entiers) quadratiques par les petites lettres de l'alphabet grec $\alpha \beta \gamma \ldots \delta \ldots \omega$ et leurs valeurs absolues suivant la coutume par $|\alpha|$, etc.

6. Le corps $k(\sqrt{m})$. *Les entiers et les bases des corps.* — Les recherches seront plus simples et plus claires si nous admettons que le nombre m est un entier rationnel sans facteur carré.

Nous ferons d'autant plus volontiers cette hypothèse, que le cas général pour m quelconque se ramène à ce cas particulier.

Tous les nombres du corps $k(\sqrt{m})$ sont de la forme

$$\frac{a + b\sqrt{m}}{c}.$$

Si m est positif le corps ne contient que les nombres réels. il est dit un *corps réel.* Si m est négatif tous les nombres de la forme $u + v\sqrt{m}$, $v \neq 0$ sont imaginaires ou complexes et $k(\sqrt{m})$ est dit un *corps imaginaire.*

A chaque nombre

$$\alpha = \frac{a + b\sqrt{m}}{c}$$

correspond le nombre conjugué

$$\alpha' = \frac{a - b\sqrt{m}}{c}$$

α et α' sont les racines d'une même opération du second degré à coefficients entiers rationnels. α' résulte de α lorsqu'on y remplace $+\sqrt{m}$ par $-\sqrt{m}$. Le nombre conjugué de α sera toujours représenté par α'. Si α est un entier des corps, α' l'est aussi et réciproquement.

Il est évident que $a + b\sqrt{m}$ est un entier.

D'une façon générale on peut mettre tout entier sous la forme

$$\frac{a + b\sqrt{m}}{c}$$

où a, b, c sont des entiers sans diviseur commun. Voyons si pour des entiers c peut prendre d'autres valeurs que $c = 1$. Le nombre α est racine de

$$x^2 - \frac{2a}{c}x + \frac{a^2 - b^2m}{c^2} = 0$$

et il n'est entier que si $\frac{2a}{c}$ et $\frac{a^2 - b^2m}{c^2}$ sont des entiers rationnels. Supposons que c admette un facteur premier $p > 2$, alors a sera divisible par p. Mais alors p^2 doit être contenu dans $a^2 - b^2m$ et comme p divise a, et que m ne contient aucun facteur carré, il faut que $b^2 \equiv 0$, p. a, b, c ne seraient pas premiers entre eux. On démontre de la même manière que c ne peut contenir 2 à une puissance supérieure à 1, par suite tous les entiers sont contenus dans

$$\frac{a + b\sqrt{m}}{2}.$$

On voit que $a = 0$, $b \not\equiv 0$, ou $a \not\equiv 0$, $b = 0$, le nombre qui n'est pas nul doit être divisible par c ou que c doit être égal à 1.

L'examen de tous les cas possibles donne le :

Théorème. — Tout entier du corps est de la forme

$$a - b\,\frac{1 + \sqrt{m}}{2}$$

lorsque $m \equiv 1$ (4), de la forme $a + b\sqrt{m}$ pour $m \equiv 2$ (4) ou $m \equiv 3$ (4) où a et b sont des entiers quelconques.

Démonstration. 1er *Cas* : $m \equiv 1$ (4). Si a et b sont des entiers quelconques le nombre $\alpha = \frac{a + b\sqrt{m}}{2}$ est entier si $\frac{2a}{2}$ et $\frac{a^2 - b^2m}{4}$ sont entiers. La première condition est toujours satisfaite, pour que la seconde le soit il faut que a et b soient tous deux pairs ou tous deux impairs

$$\alpha = \frac{2a_1 + 2b_1\sqrt{m}}{2} = a_1 + b_1\sqrt{m}$$

$$\alpha = \frac{(2a_1 + 1) + (2b_1 + 1)\sqrt{m}}{2} = a_2 + b_2\frac{1 + \sqrt{m}}{2}$$

ces deux expressions sont contenues dans la formule

$$a + b\frac{1 + \sqrt{m}}{2}$$

et l'on voit immédiatement que cette formule ne peut représenter que des nombres entiers.

2e *Cas* : $m \equiv 2$ (4), $m \equiv 3$ (4), $\alpha = \frac{a + b\sqrt{m}}{2}$ est entier si $a^2 - b^2m \equiv 0$ (4), comme le carré d'un entier $\equiv 0$, ou $\equiv 1$ (4), il faut que a et b soient tous deux pairs. Tous les entiers du corps sont de la forme $a + b\sqrt{m}$.

Posons donc

$$\omega = \frac{1 + \sqrt{m}}{2} \quad \text{lorsque} \quad m \equiv 1 \ (4)$$

$$\omega = \sqrt{m} \quad \text{pour} \quad m \not\equiv 1 \ (4)$$

tout entier des corps $k(\sqrt{m})$ pourra être représenté par une expression linéaire

$$a \cdot 1 + b\omega$$

où a et b sont des entiers rationnels quelconques.

Nous dirons que les nombres 1 et ω forment une base du corps.

Définition. — On dit que deux nombres ω_1, ω_2 d'un corps quadratique forment une base, si tout nombre du corps peut être mis sous la forme

$$a\omega_1 + b\omega_2$$

et cela d'une seule manière, a et b étant des entiers rationnels bien déterminés.

On peut choisir comme base une infinité de couples ω_1, ω_2. En effet si ω_1, ω_2 sont deux entiers du corps, on a

$$\omega_1 = a_1 + b_1\omega$$
$$\omega_2 = a_2 + b_2\omega$$

et $\omega_1\omega_2$ formeront une base si l'on a

$$\begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix} = \pm 1$$

car on a alors

$$1 = \frac{b_2\omega_1 - b_1\omega_2}{\pm 1} \qquad \omega = \frac{-a_2\omega_1 + a_1\omega_2}{\pm 1}$$

et on a pour tout entier α^* la représentation

$$\alpha^* = a^*\omega_1 + b^*\omega_2.$$

D'autre part on obtient tous les entiers du corps en donnant à a et b toutes les valeurs possibles.

On peut satisfaire à

$$a_1b_2 - a_2b_1 = \pm 1$$

pour une infinité de système de valeurs de a_1b_1, a_2b_2, il suffit de choisir a_1b_1 quelconques mais premiers entre eux et de déterminer a_2b_2 satisfaisant à l'équation précédente.

Il y a donc une infinité de couples de nombres de base

Théorème. — Si $\omega_1\omega_2$ et $\omega_1^*\omega_2^*$ sont deux bases différentes d'un corps et si l'on a

$$\omega_1^* = a_1\omega_1 + b_1\omega_2$$
$$\omega_2^* = a_2\omega_1 + b_2\omega_2,$$

on a aussi

$$a_1b_2 - a_2b_1 = \pm 1.$$

On le démontre en écrivant $\omega_1\omega_2$ en fonction de $\omega_1^*\omega_2^*$. Nous allons déduire maintenant les résultats suivants.

Théorème. — La somme, la différence, le produit de deux nombres entiers α et β des corps est un nombre entier.

Démonstration : Soient deux nombres

$$\alpha = a + b\omega$$
$$\beta = c + d\omega$$
$$\alpha \pm \beta = a \pm c + (b \pm d)\,\omega$$

et ce nombre satisfait aux conditions des entiers, comme α et β eux-mêmes. Quant au produit nous distinguerons deux cas

1. $m \equiv 1\ (4)$ $\quad \alpha\,.\,\beta = ac + (ad + bc)\,\omega + bd\omega^2$

$$\omega^2 = \frac{1 + 2\sqrt{m} + m}{4} = \frac{m - 1}{4} + \omega$$

donc $\alpha\,.\,\beta$ est bien de la forme $u + v\omega$, où u et v sont des entiers rationnels, c'est-à-dire $\alpha\,.\,\beta$ est un entier

2. $m \not\equiv 1\ (4)$ $\quad \alpha\,.\,\beta = ac + bdm + (ad + bc)\,\omega$

par suite $\alpha\,.\,\beta$ est de la forme $u + v\omega$ il est entier.

Soient des nombres $\alpha, \beta, \gamma, \ldots$ et appliquons leur l'addition, la soustraction, la multiplication dans un ordre quelconque et aussi souvent qu'il nous plaira nous aurons des nombres entiers, c'est ce que nous exprimerons ainsi :

Théorème. — Toute fonction rationnelle entière de nombres entiers $\alpha, \beta, \gamma, \ldots$ du corps $k(\sqrt{m})$ avec des coefficients rationnels entiers est un nombre entier.

Introduisons quelques notions qui nous seront utiles.

La norme d'un nombre α : $n(\alpha) = \alpha\alpha'$ c'est-à-dire le produit de α par son conjugué α'. La norme d'un nombre entier est un nombre entier rationnel, elle est égale au terme tout connu de l'équation à laquelle satisfait α.

Théorème. — La norme d'un produit de deux nombres est égal au produit de leurs normes.

$$n(\alpha\beta) = \alpha\beta\,.\,\alpha'\beta' = \alpha\alpha'\,.\,\beta\beta' = n(\alpha)\,.\,n(\beta).$$

Le discriminant d'un nombre α est $d(\alpha) = (\alpha - \alpha')^2$, ce nombre est aussi un entier rationnel. Le discriminant d'un nombre rationnel est toujours égal à zéro.

Le discriminant du corps k est l'expression

$$d = d(\omega) = (\omega - \omega')^2$$

que l'on peut écrire

$$d = \begin{vmatrix} 1 & \omega \\ 1 & \omega' \end{vmatrix}^2$$

et l'on voit facilement que si ω_1 ω_2 sont deux nombres formant une autre base

$$d = \begin{vmatrix} \omega_1 & \omega_2 \\ \omega'_1 & \omega'_2 \end{vmatrix}^2$$

car on a

$$\omega_1 = a_1 + b_1\omega \qquad \omega'_1 = a_1 + b_1\omega'$$
$$\omega_2 = a_2 + b_2\omega \qquad \omega'_2 = a_2 + b_2\omega'$$

et

$$\begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix} = \pm 1$$

et d'après le théorème sur la multiplication des déterminants

$$\begin{vmatrix} \omega_1 & \omega_2 \\ \omega'_1 & \omega'_2 \end{vmatrix} = \begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix} \begin{vmatrix} 1 & \omega \\ 1 & \omega' \end{vmatrix}$$

et par suite

$$d = \begin{vmatrix} \omega_1 & \omega_2 \\ \omega'_1 & \omega'_2 \end{vmatrix}^2 = \begin{vmatrix} 1 & \omega \\ 1 & \omega' \end{vmatrix}^2.$$

Le discriminant du corps $k(\sqrt{m})$ est

1. $d = m$ pour $m \equiv 1 \ (4)$
2. $d = 4m$ pour $m \not\equiv 1 \ (4)$.

Le discriminant est positif pour les corps réels, négatif pour les corps imaginaires. Il n'est impair que si $m \equiv 1 \ (4)$.

Exemples numériques : m ne doit contenir aucun facteur carré, nous pourrons prendre

$$m = \pm 1 \pm 2 \pm 3 \pm 5 \pm 6 \pm 7 \pm 10 \pm 11 \pm 13 \ldots$$

Le corps $k(\sqrt{1})$ est le corps des nombres rationnels, nous ne nous en occuperons pas ici.

1er EXEMPLE $k(\sqrt{-1})$.

$m = -1$, $m \equiv 3\ (4)$, on peut prendre pour base $1, \omega = \sqrt{-1}$.

Les entiers sont de la forme $a + b\sqrt{-1}$.

Le conjugué d'un nombre $a + b\sqrt{-1}$ est $a - b\sqrt{-1}$ sa norme $a^2 + b^2$.

Le discriminant d'un nombre α du corps est $d(\alpha) = -4b^2$.

Il y a un nombre qui joue un rôle particulier c'est $\varepsilon = \sqrt{-1}$ $n(\varepsilon) = +1$, $\frac{1}{\varepsilon}$ est donc un nombre entier et l'on peut bien dire que $\sqrt{-1}$ est un nombre entier qui divise ± 1.

Le discriminant du corps est -4.

On peut prendre une autre base du corps que $1, \sqrt{-1}$ par exemple

$$\omega_1 = 1 + \sqrt{-1}\ (= 1 \,.\, 1 + 1\omega) \qquad \omega_2 = 2 + \sqrt{-1}\ (= 2 \,.\, 1 + 1 \,.\, \omega)$$

car alors

$$a_1 b_2 - a_2 b_1 = 1$$

ou encore

$$\omega_1 = 1 - \sqrt{-1} \qquad \omega_2 = -2 + 3\sqrt{-1}$$

où

$$a_1 b_2 - a_2 b_1 = 1, \quad \text{etc.}$$

2^e^ EXEMPLE $k(\sqrt{5})$.

Soit $m = 5$, $m \equiv 1\ (4)$, on peut prendre pour base $1, \omega = \frac{1 + \sqrt{5}}{2}$ ou $1, \omega'$, car $\omega' = 1 - \omega$, ou $2 + 3\omega$, $1 + 2\omega$, etc.

Les nombres entiers sont de la forme

$$a + b\omega = a + b\,\frac{1 + \sqrt{5}}{2}.$$

Le conjugué de

$$\alpha = a + b\omega$$

est

$$a + b\omega' = a + b\,\frac{1 - \sqrt{5}}{2}$$

et l'on a

$$n(\alpha) = a^2 + ab - b^2$$

le discriminant

$$d(\alpha) = 5b^2$$

Dans l'exemple précédent $\sqrt{-1}$ jouerait un rôle particulier, ici c'est ω. On a effet $n(\omega) = -1$ et par suite ω et ω' divisent ± 1. Il en est de même de $\omega^2 \omega^3 \ldots \omega^{-1}\ \omega^{-2}\ \omega^{-3} \ldots$ qui diffèrent les uns des autres et de ω.

Le discriminant du corps est 5.

Nous réunissons dans un tableau les résultats relatifs à d'autres nombres d'ailleurs une table plus importante se trouve à la fin de l'ouvrage.

Corps	Caractères de m	Base	Nombres entiers	$n(\alpha)$	$d(\alpha)$	d
$k(\sqrt{5})$	$5 \equiv 1, (4)$	$1, \frac{1+\sqrt{5}}{2}$	$a + b\frac{1+\sqrt{5}}{2}$	$a^2 + ab - b^2$	$5\,b^2$	5
$k(\sqrt{3})$	$3 \equiv 3, (4)$	$1, \sqrt{3}$	$a + b\sqrt{3}$	$a^2 - 3b^2$	$12\,b^2$	12
$k(\sqrt{2})$	$2 \equiv 2, (4)$	$1, \sqrt{2}$	$a + b\sqrt{2}$	$a^2 - 2b^3$	$8\,b^2$	8
$k(\sqrt{-1})$	$-1 \equiv 3, (4)$	$1, \sqrt{-1}$	$a + b\sqrt{-1}$	$a^2 + b^2$	$-4\,b^2$	-4
$k(\sqrt{-2})$	$-2 \equiv 2, (4)$	$1, \sqrt{-2}$	$a + b\sqrt{-2}$	$a^2 + 2b^2$	$-8\,b^2$	-8
$k(\sqrt{-3})$	$-3 \equiv 1, (4)$	$1, \frac{1+\sqrt{-3}}{2}$	$a + b\frac{1+\sqrt{-3}}{2}$	$a^2 + ab + b^2$	$-3\,b^2$	-3

On voit d'après ce tableau que le discriminant du corps est toujours le plus grand commun diviseur des nombres entiers du corps. Les discriminants des nombres rationnels et ceux-là seulement sont nuls.

La norme d'un nombre entier dans un corps réel peut être positive ou négative, dans un corps imaginaire elle est toujours positive. Dans tous les cas la norme d'un nombre différent de zéro est toujours en valeur absolue $\geqq 1$.

7. Divisibilité des nombres entiers. — On dit qu'un nombre entier α du corps $k(\sqrt{m})$ est divisible par un autre nombre entier β de corps, lorsqu'on peut trouver un autre nombre γ ; tel que

$$\alpha = \beta\gamma.$$

Soit π un nombre qui ne divise pas $\pm$ 1 et qui n'est divisible que par lui-même ou par des diviseurs de $\pm$ 1, π présente les mêmes caractères qu'un nombre premier rationnel, nous dirons provisoirement que π est un nombre *indécomposable.*

Supposons qu'on ait décomposé un nombre en un produit de facteurs indécomposables, une question se pose : cette décomposition n'est-elle possible que d'une seule manière, ou peut-on avoir

$$\alpha = kk_1 \ldots k_n = \pi_1 \pi_2 \ldots \pi_n$$

où les k sont tels qu'aucun d'eux ne soit divisible par un des π et ne s'en distingue pas uniquement par des facteurs de l'unité.

On essaiera de transporter l'algorithme d'Euclide dans le domaine des nombres quadratiques. Si cet essai réussit on en conclura que la décomposition n'est possible que d'une seule manière. Si au contraire cet essai nous montre que l'algorithme n'est plus possible la décomposition unique restera douteuse.

Pour mieux nous faire comprendre, prenons d'abord un exemple et choisissons le tel que le procédé d'Euclide s'applique. Soit le corps $k(\sqrt{-1})$.

Soient

$$\alpha = a_1 + a_2 \sqrt{-1}, \qquad \beta = b_1 + b_2 \sqrt{-1}$$

deux nombres entiers et soit $n(\alpha) \geqq n(\beta)$ et tels que α ne contienne pas exactement β. La division $\frac{\alpha}{\beta}$ donne

$$\frac{\alpha}{\beta} = \frac{\alpha\beta'}{n(\beta)} = \gamma + \frac{r + s\sqrt{-1}}{n(\beta)}$$

mais ce reste est indéterminé en ce sens que r et s peuvent être compris entre o et $n(\beta)$ ou entre o et $-n(\beta)$ ou enfin entre

$$-\frac{1}{2}n(\beta) \quad \text{et} \quad +\frac{1}{2}n(\beta).$$

Nous admettrons que l'on prend comme reste « le reste qui a la plus petite valeur absolue » avec la condition

$$|r| \leqq \frac{1}{2}n(\beta) \qquad |s| \leqq \frac{1}{2}n(\beta)$$

on pourra écrire alors

$$\alpha = \beta\gamma + \rho_0$$

ou

$$\rho_0 = \frac{r + s\sqrt{-1}}{\beta}$$

est un nombre entier tel que

$$n(\rho_0) = \frac{r^2 + s^2}{n(\beta)} \leqq \frac{1}{2} n(\beta) .$$

Si $n(\rho_0) > 1$ on divisera β par ρ_0, soit

$$\beta = \gamma_1\rho_0 + \rho_1$$

avec la condition

$$n(\rho_1) \leqq \frac{1}{2} n(\rho_0)$$

on continuera jusqu'à ce que $n(\rho_{n-1})$ étant > 1 on ait $n(\rho_n) = 0$ ou $n(\rho_n) = 1$. Les normes allant en diminuant on atteindra toujours l'un de ces résultats. Dans le cas $\rho_n = 0$, α et β admettent pour diviseur commun ρ_{n-1} dans le second cas $n(\rho_n) = 1$ ρ_n divise l'unité, α et β n'ont d'autres diviseurs commun que 1 ou des nombres qui divisent 1, nous dirons qu'ils sont premiers entre eux.

Il résulte de ces considérations que l'algorithme d'Euclide s'applique, car on arrive à ρ_n au bout d'un nombre limité d'opérations. On peut encore affirmer que dans le corps $k(\sqrt{-1})$ la décomposition en facteurs n'est possible que d'une seule manière. Prenons le cas général de $k(\sqrt{m})$ pour $m \not\equiv 1 \ (4)$ et posons

$$\frac{\alpha}{\beta} = \frac{\alpha \cdot \beta'}{n(\beta)} = \gamma + \frac{r + s\sqrt{m}}{n(\beta)}$$

ou

$$\alpha = \gamma\beta + \rho_0 ;$$

appelons « reste minimum en valeur absolue »

$$|r| \leqq \frac{1}{2} n(\beta) \quad |s| \leqq \frac{1}{2} |n(\beta)|$$

nous aurons

$$n(\rho_0) = \frac{r^2 - s^2 m}{n(\beta')}$$

$$|\, n(\rho_0) \,| \leqq |\, n(\beta) \,| \left| \frac{1}{4} + \frac{m}{4} \right|$$

on ne peut conclure de là

$$|\, n(\rho_0) \,| < n(\beta)$$

que si $3 > m > -3$. Dans tous les autres cas il peut arriver que $|\, n(\rho_0) \,| > n(\beta)$, etc., et alors il n'est pas évident que la recherche du plus grand commun diviseur comporte un nombre limité d'opérations. Et c'est là le cas général pour les nombres d'un corps $k(\sqrt{m})$. C'est donc que pour ces corps on ne peut plus fonder la décomposition unique sur la méthode d'Euclide et nous ne pouvons plus rien affirmer.

On trouverait un résultat analogue pour $m \equiv 1\ (4)$.

Nous allons d'ailleurs montrer par des exemples particuliers qu'il est possible de décomposer les nombres de certains corps de plusieurs manières en un produit de facteurs.

1er Exemple. — Soit le corps $k(\sqrt{-5})$.

Les nombres entiers de ce corps sont de la forme $a + b\sqrt{-5}$ Les seuls nombres des corps qui divisent 1 ou dont la norme est 1 sont ± 1 car si

$$1 = (a + b\sqrt{-5})\,(a_1 + b_1\sqrt{-5})$$

en passant aux normes

$$1 = (a^2 + 5\,b^2)\,(a_1^2 + 5\,b_1^2)$$

et comme

$$a^2 + 5\,b^2,\ a_1^2 + 5\,b_1^2$$

sont des nombres entiers, on a

$$1 = a^2 + 5\,b^2 = a_1^2 + 5\,b_1^2$$

c'est-à-dire

$$a = a_1 = \pm 1, \qquad b = b_1 = 0.$$

Soit le nombre 21

$$21 = 3.7 = (4 + \sqrt{-5})(4 - \sqrt{-5}) = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5})$$

où les nombres entiers

$$3,\ 7,\ 4 + \sqrt{-5},\quad 4 - \sqrt{-5},\quad 1 + 2\sqrt{-5},\quad 1 - 2\sqrt{-5}$$

sont des nombres indécomposables, essentiellement différents car si on avait

$$3 = (a + b\sqrt{-5})(a_1 + b_1\sqrt{-5})$$

il en résulterait

$$3 = aa_1 - 5\,bb_1$$
$$0 = ab_1 + a_1b,$$

on pourrait poser

$$a_1 = \mathrm{P}.a, \qquad b_1 = -\mathrm{P}.b$$

et par suite

$$3 = \mathrm{P}a^2 + 5\mathrm{P}b^2$$

où $\mathrm{P}a^2$ $\mathrm{P}b^2$ sont des entiers non négatifs, pour $b \neq 0$. $5\mathrm{P}b^2 > 3$ la dernière égalité est impossible. On a donc

$$3 = \mathrm{P}a^2 \qquad 0 = \mathrm{P}b^2$$

ou

$$\begin{cases} b = 0 & a = 3 & \mathrm{P} = \frac{1}{3} \\ b_1 = 0 & a_1 = 1 \end{cases}$$

ou

$$\begin{cases} b = 0 & a = 1 \\ b_1 = 0 & a_1 = 3 \end{cases}$$

c'est-à-dire qu'il vient $3 = 3.1 = 1.3$, 3 ne peut être décomposé.

Supposons que $4 + \sqrt{-5}$ soit décomposable et soit de la forme

$$4 + \sqrt{-5} = (a + b\sqrt{-5})(a_1 + b_1\sqrt{-5})$$

en formant les normes on aurait

$$21 = (a^2 + 5\,b^2)(a_1^2 + 5\,b_1^2)$$

les nombres de cette égalité étant tous rationnels, il reste les cas suivants :

(1) $$21 = a^2 + 5b^2, \qquad 1 = a_1^2 + 5b_1^2$$

avec les solutions

(a) $$a = 4, \quad b = 1, \quad a_1 = \pm 1, \quad b_1 = 0$$

qui ne satisfait pas à l'équation primitive, et les solutions

(b) $$a = 1, \quad b = 2, \quad a_1 = \pm 1, \quad b_1 = 0$$

(2) $$3 = a^2 + 5b^2, \qquad 7 = a_1^2 + 5b_1^2$$

qui est impossible, ainsi que

(3) $$a_1^2 + 5b_1^2 = 3, \qquad a^2 + 5b^2 = 7.$$

On verrait de même que 7

$$1 + 2\sqrt{5}, \qquad 1 - 2\sqrt{5}$$

sont indécomposables.

Il reste à démontrer que ces décompositions sont essentiellement différentes, c'est-à-dire qu'ils ne diffèrent pas des facteurs diviseurs de l'unité.

Supposons que l'on ait par exemple

$$4 + \sqrt{-5} = (1 + 2\sqrt{-5})(x + y\sqrt{-5})$$

on aurait

$$4 = x - 10y$$
$$1 = 2x + y$$

c'est-à-dire

$$x = \frac{2}{3}, \quad y = -\frac{1}{3}$$

donc $4 + \sqrt{-5}$ n'est pas divisible par $1 + 2\sqrt{-5}$ de même pour les autres. Dans le même corps on a des décompositions plus simples

$$6 = 2.3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$
$$9 = 3.3 = (2 + \sqrt{-5})(2 - \sqrt{-5}).$$

Cet exemple montre qu'il y a des nombres que l'on peut décom-

poser de plusieurs manières en un produit de facteurs. La notion de « nombre indécomposable » n'est pas du tout identique à la notion des nombres premiers rationnels.

2e Exemple. — Considérons le corps réel $k(\sqrt{10})$.

Les nombres qui nous intéressent tout d'abord sont les diviseurs de ± 1. Soit ε un pareil nombre

$$\pm 1 = \varepsilon . \varepsilon_1 \quad \text{on a} \quad p = n(\varepsilon)\, n(\varepsilon_1)$$

comme la norme d'un nombre entier est un entier rationnel, on a

$$n(\varepsilon) = \pm 1. \quad n(\varepsilon_1) = \pm 1.$$

Il est donc indifférent de dire qu'un nombre divise l'unité ou que sa norme $= \pm 1$.

Si $\varepsilon = a + b\sqrt{10}$ nous avons à déterminer a et b de telle sorte que

$$\pm 1 = a^2 - 10 b^2$$

on voit immédiatement que $-1 = a^2 - 10 b^2$ admet la solution

$$a = \pm 3. \quad b = \pm 1$$

et l'on a

$$-1 = (3 + \sqrt{10})\,(3 - \sqrt{10})$$
$$-1 = (-3 + \sqrt{10})\,(-3 - \sqrt{10}).$$

On peut déduire de ces égalités bien d'autres solutions

Elevons au carré

$$1 = (19 + 6\sqrt{10})\,(19 - 6\sqrt{10})$$

qui donne pour

$$1 = a^2 - 10 b^2$$

la solution

$$a = 19. \quad b = 6.$$

D'une façon analogue toute puissance entière

$$(-1)^n = (3 + \sqrt{10})^n\,(3 - \sqrt{10})^n$$

donne une solution de

$$(-1)^n = a^2 - 10 b^2$$

les nombres

$$3 + \sqrt{10}, \quad -3 + \sqrt{10}, \quad 19 + 6\sqrt{10}, \text{ etc.}$$

sont des diviseurs non seulement de l'unité mais de tout entier du corps.

Nous ne considérerons pas les décompositions

$$6 = 2.3$$

et

$$6 = -2.3\,(3 + \sqrt{10})\,(3 - \sqrt{10})$$

comme différentes.

Avec cette restriction 2 et 3 sont indécomposables, la décomposition

$$-4 = (6 + 2\sqrt{10})\,(6 - 2\sqrt{10})$$

n'est pas essentiellement différente de $4 = 2 \times 2$, par contre nous compterons

$$2 \,.\, 3 = (4 + \sqrt{10})\,(4 - \sqrt{10}) = 6$$

comme deux décompositions différentes de b_1 tandis que les décompositions

$$6 = (4 + \sqrt{10})\,(4 - \sqrt{10})$$
$$6 = (16 + 5\sqrt{10})\,(16 - 5\sqrt{10})$$

sont égales entre elles, car les nombres

$$4 + \sqrt{10}, \qquad 16 - 5\sqrt{10}$$

d'une part, et les nombres

$$4 - \sqrt{10} \quad \text{et} \quad 16 + 5\sqrt{10}$$

d'autre part ne diffèrent que par un facteur diviseur de l'unité. On a par exemple

$$(4 + \sqrt{10})\,(19 - 6\sqrt{10}) = 16 - 5\sqrt{10}.$$

Ce dernier cas nous montre que deux décompositions en apparence très différentes peuvent en réalité être identiques grâce aux diviseurs de l'unité. Il nous reste cependant ce fait que le nombre

6 dans le corps $k(\sqrt{10})$ peut être décomposé de plusieurs manières. On peut le montrer également pour une infinité d'autres nombres.

Il ne peut plus être question de démontrer le théorème fondamental de la théorie des nombres rationnels — et les lois de la théorie des nombres rationnels ne peuvent se généraliser — Gauss et Kummer (1844) avaient vu cette difficulté. Kummer inventa un artifice pour y remédier. Pour rétablir le théorème de la décomposition unique il imagina le concept des *nombres idéaux* (1). C'est une des plus belles découvertes de la théorie des nombres. Il serait tentant de donner ici la représentation des nombres idéaux d'après Kummer, nous passerons cependant de suite à la notion d'*idéal* tel que l'a donnée M. Dedekind (2). Il l'a tiré du concept des nombres idéaux, et a donné à l'idée première une coexistence plus sensible.

8. Systèmes particuliers de nombres idéaux. — On peut expliquer le concept des idéaux par un cas tout particulier. Au lieu de considérer le domaine des nombres entiers rationnels tout entier, n'en considérons qu'une partie, par exemple l'ensemble (3) des nombres de la forme $4n + 1$, on peut former le produit de deux quelconques de ces nombres et on peut définir la division comme d'ordinaire, tandis qu'il faut abandonner l'addition et la soustraction.

Soit la suite

$$1,\ 5,\ 9,\ 13,\ 17,\ 21,\ 25,\ \ldots\ 73,\ 77,\ \ldots\ 141$$

le produit de deux nombres quelconques de la suite fait encore partie de la suite

$$(4n + 1)(4n_1 + 1) = 4m + 1$$
$$(\text{Exemple } 5 \cdot 9 = 45,\ 9 \cdot 13 = 117 \ldots)$$

---

(1) *Journal de Crelles*, t. XXXV, p. 319 et ibid. p. 317. Les développements de Kummer sont relatifs au Kreiskörper (Bei der K. Akad. Berlin, mars 1845). Voir Bachmann. — *Théorie des nombres*, t. V, p. 144; il parle des nombres idéaux du corps quadratique.

(2) Vorlesungen Suppl. XI, p. 550 (Modul. S. 493).

(3) M. Fueter dans le *Journal de Crelle*, t. 130, p. 208 donne à un pareil système le nom de faisceau de nombres.

et dans un produit on peut intervertir l'ordre des facteurs.

Les nombres

$$5, \quad 9, \quad 13, \quad 17, \quad 21, \quad 29 \quad \ldots$$

sont indécomposables dans le domaine des nombres considérés, car 21 par exemple ne peut être considéré comme le produit de deux autres nombres de la suite. Par contre

$$10\,857 = 141 \cdot 77 = 21 \cdot 517$$

peut être décomposé de deux manières, et ces deux manières sont essentiellement distinctes, car 21, 77, 141, 517 sont indécomposables.

De même

$$693 = 21 \cdot 23 = 9 \cdot 77$$
$$441 = 21^2 = 9 \cdot 49$$

et ainsi de suite.

Mais nous savons d'avance comment il faudra nous y prendre pour rendre cette décomposition unique. Si à tous ces nombres on ajoute tous les nombres rationnels, on a par exemple

$$10857 = 3 \cdot 7 \cdot 11 \cdot 47$$

et cette décomposition est unique dans le domaine ainsi étendu. L'idée de Kummer appliquée au cas particulier consiste à adjoindre aux nombres du corps ces facteurs élémentaires 3, 7, 11, 47 comme nombres idéaux. Le nombre 3 peut être considéré comme le plus grand commun diviseur de 21 et de 141, 7 comme celui de 77 et 21, 11 celui de 77 et de 517 ; 47 de 141 et de 517.

Si donc nous désignons par le symbole Idéal $j = (a, b)$, précisément le plus grand diviseur des deux entiers a et b, le facteur 3 de l'exemple précédent devient identique au symbole (21, 141), de plus 7 est identique à (21,77) et de même 11, 47 sont identiques, l'un à (77, 517), l'autre à (141, 517). Si nous y ajoutons le symbole $j = (a)$, nous écrirons

$$(141) = (21,141)\,(141,517) \quad ; \quad (77) = (21,77)\,(77,517)$$

et

$$(10857) = (21,141)\,(141,517)\,(77,21)\,(77,517)$$

Comme d'autre part

$$(21) = (21, 141)(21, 77)$$

et que

$$517 = (517, 77)(517, 141)$$

on voit que 141 . 77 et 21 . 517 donnent les mêmes décompositions. On procède d'une façon analogue pour les autres exempels.

$$(693) = (21, 9)(21, 77)(33, 9)(33, 77)$$
$$(441) = (21, 9)(21, 49)(21, 9)(21, 49).$$

De la définition du symbole a, b, on tire la conclusion suivante : le symbole (a, b) conserve la même signification, si on lui adjoint un nombre quelconque de la forme $ac + bd$, où c et d sont deux nombres quelconques du système donné de nombres, c'est-à-dire que (a, b), $(a, b, ac, bd \ldots)$ représentent le même idéal.

On peut donc tout aussi bien définir un idéal comme un système simultané d'un *nombre quelconque* de nombres, c'est-à-dire comme le plus grand commun diviseur des nombres de ce système, et il suffit de développer un critère concernant l'égalité de deux idéaux. Dans l'exemple numérique on reconnait immédiatement que

Deux idéaux sont égaux, lorsque tout nombre du premier se retrouve dans le second, ou lorsqu'il peut être obtenu par une combinaison linéaire des nombres du second à l'aide de nombres appropriés appartenant au domaine considéré.

Examinons maintenant le cas général.

9. Les idéaux du corps quadratique. — On adjoint aux nombres entiers du corps une infinité d'*idéaux* ainsi définis.

Définition. — On appelle idéal du corps $k(\sqrt{m})$ et on désigne par

$$j = (\alpha, \beta, \gamma, \ldots)$$

un système de nombres tels que toute combinaison linéaire

$$\alpha\lambda + \beta\mu + \gamma\nu + \ldots,$$

des nombres $\alpha, \beta, \gamma \ldots$ faite au moyen de nombres entiers

λ, μ, ν ... pris dans le corps, appartienne encore au système. On le désigne par

$$j = (\alpha, \beta, \gamma, \ldots).$$

En particulier un idéal est dit un *idéal principal*, lorsque ses nombres sont des multiples d'un nombre entier du corps appartenant à l'idéal, c'est-à-dire s'il est de la forme

$$j = (\alpha, \alpha\lambda, \alpha\mu, \ldots)$$

on écrit alors simplement $j = (\alpha)$.

Il nous faudra bientôt discerner exactement les idéaux, les idéaux principaux et les nombres, mais il nous arrivera souvent d'employer l'expression nombre au lieu de l'expression idéal principal sans qu'il y ait pour cela ambiguité.

Des idéaux qui ne sont pas des idéaux principaux nous dirons qu'ils sont des idéaux *non principaux*.

Lorsqu'un idéal contient 1 ou un nombre contenu dans 1, nous dirons qu'il est un *idéal unité* et nous le désignerons par le symbole $j = (1)$.

En ce qui concerne les notations nous conviendrons, d'employer toujours les lettres allemandes $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$, $\mathfrak{d}$ ... $\mathfrak{n}$ ... pour désigner des idéaux. Avant d'employer les idéaux nous poserons la définition. Un idéal est donné lorsqu'on connait soit un, soit deux, soit trois nombres déterminés du corps, et on écrit l'idéal (α) ou (α, β) ou (α, β, γ) en négligeant de mettre des points dans les parenthèses.

Définition. — Deux idéaux $(\alpha, \beta, \gamma, \ldots)$ et $(\alpha_1, \beta_1, \gamma_1, \ldots)$ du corps $k(\sqrt{m})$ sont égaux

$$(\alpha, \beta, \gamma) = (\alpha_1, \beta_1, \gamma_1 \ldots)$$

si tout nombre α du premier idéal appartient au second (ou s'il peut être exprimé par une combinaison linéaire $\alpha_1\lambda + \beta_1\mu \ldots$) et réciproquement si chaque nombre $\alpha_1\beta_1$ ... du second appartient au premier.

Quant à la multiplication des idéaux nous poserons :

Définition. — Soient

$$\mathfrak{a} = (\alpha, \beta, \gamma \ldots) \quad \text{et} \quad \mathfrak{b} = (\alpha_1, \beta, \gamma \ldots)$$

deux idéaux du corps $k(\sqrt{m})$, on entend par produit de ces deux

idéaux, l'idéal formé de tous les nombres obtenus en multipliant tous les nombres de $\mathfrak{a}$ par tous les nombres de $\mathfrak{b}$ et si l'on ajoute encore à ce système toutes les combinaisons linéaires de ces produits avec des entiers du corps.

$$\mathfrak{ab} = (\alpha\alpha_1,\ \alpha\beta_1,\ \alpha\gamma_1 \ldots \alpha_1\beta,\ \beta\beta_1 \ldots \gamma\gamma_1 \ldots)$$

De cette définition, résulte immédiatement

$$\mathfrak{ab} = \mathfrak{ba}$$

et par suite on a pour la division :

Un idéal $\mathfrak{a}$ est dit divisible par un idéal $\mathfrak{b}$, lorsqu'on peut trouver un idéal $\mathfrak{c}$ tel que

$$\mathfrak{a} = \mathfrak{bc}$$

et $\mathfrak{c}$ est dit le quotient de $\mathfrak{a}$ par $\mathfrak{b}$.

Les concepts de la multiplication et de la division des nombres entiers peuvent s'étendre aux idéaux, les concepts d'addition et de soustraction ne peuvent être généralisés.

Théorème. — Dans tout idéal d'un corps $k(\sqrt{m})$ on peut trouver d'une infinité de manières deux nombres entiers du corps $\iota_1^*\ \iota_2^*$ tels que tout nombre de l'idéal puisse être mis sous la forme

$$l_1\iota_1^* + l_2\iota_2^*$$

où $l_1 l_2$ sont des entiers rationnels.

Démonstration : Nous écrirons l'idéal j en exprimant tous ses nombres au moyen de la base du corps $1, \omega$.

$$\mathfrak{j} = (a + b\omega, \quad a_1 + b_1\omega, \quad a_2 + b_2\omega + \ldots \mathrm{A} \ldots)$$

et nous démontrerons tout d'abord : que si $a + b\omega$, $a_1 + b_1\omega$ sont deux nombres de l'idéal, il y a aussi dans cet idéal un nombre $a' + b'\omega$ tel que b' est le plus grand commun diviseur de b et de b_1. En effet la définition d'un idéal nous montre que tout nombre

$$x(a + b\omega) + y(a_1 + b\omega)$$

appartient à l'idéal si x et y représentent des nombres entiers. Mais on peut déterminer x et y de façon à satisfaire à

$$xb + yb_1 = b'.$$

En répétant ce raisonnement pour $a' + b'\omega$ et $a_2 + b_2\omega$ et ainsi de suite, on voit qu'il existe dans l'idéal un nombre

$$J + i_2\omega$$

tel que i_2 soit le plus grand commun diviseur de $b, b_1, b_2 \ldots$ et où J est un entier satisfaisant à certaines conditions bien déterminées. Les nombres $\frac{b}{i_2}, \frac{b_1}{i_2} \ldots$ sont tous des nombres rationnels entiers d'où il résulte que les entiers rationnels

$$a + b\omega - \frac{b}{i_2}(J + i_2\omega) = - \frac{b}{i_2} J, \text{ etc.}$$

appartiennent aussi à l'idéal. Un idéal contient donc autant d'entiers rationnels que l'on veut, ce qui est d'ailleurs évident *a priori*, car outre le nombre α l'idéal contient $n(\alpha) = \alpha\alpha'$. Soit maintenant i le plus grand commun diviseur des entiers contenus dans l'idéal, i appartient à l'idéal, on le montre comme on l'a fait précédemment pour les nombres b, b_1 et b', choisissons alors l'entier rationnel v tel que

$$0 \leqq i_1 = J - vi < i.$$

$J + i_2\omega - vi = i_1 + i_2\omega$ est un nombre de l'idéal et alors

$$\iota_1 = i, \qquad \iota_2 = i_1 + i_2\omega$$

seront deux nombres satisfaisant à la question.

Car soit $a + b\omega = \alpha$ un nombre quelconque de l'idéal $l_2 = \frac{b}{i_2}$ est entier, l'idéal contient aussi

$$\alpha - l_2\iota_2 = a - l_2 i_1$$

qui est entier et rationnel et par suite $= l_1 i$ où l_1 est un entier rationnel, on a en somme

$$\alpha = l_1 i + l_2\iota_2 = l_1\iota_1 + l_2\iota_2$$

ce qu'il fallait démontrer.

On peut donc représenter l'idéal sous la forme

$$\mathfrak{j} = (i, i_1 + i_2\omega)$$

et nous appellerons dorénavant cette représentation *la représentation canonique.*

De ce qui précède nous conclurons quelques rapports entre les nombres i, i_1 i_2. Quels que soient les nombres entiers rationnels x et y

$$x i\omega + y(i_1 + i_2\omega) = y i_1 + (x i + y i_2)\omega$$

appartient à l'idéal si x et y sont entiers et par suite

$$x i + y i_2 \equiv 0 \ (i_2)$$

i est un multiple de i_2 comme de plus

$$\omega'(i_1 + i_2\omega) = i_2\omega\omega' + i_1\omega'$$

appartient à l'idéal i_1 est un multiple de i_2.

La norme de tout nombre quadratique α appartenant à l'idéal est donc divisible par i.

Les nombres $i_1 = i$, $i_2 = i_1 + i_2\omega$ ou d'une façon générale deux nombres ι_1 ι_2 de l'idéal, qui satisfont aux conditions de l'énoncé, forment ce que l'on appelle une base de l'idéal, analogue à la base du corps.

D'une base $\iota_1\iota_2$ on peut d'une infinité de manières, déduire une autre base $i_1^* i_2^*$

$$i_1^* = a_1\iota_1 + b_2\iota_2$$
$$i_2^* = b_1\iota_1 + b_2\iota_2$$

où $a_1 a_2$, $b_1 b_2$ sont des nombres entiers, choisis de telle sorte que

$$a_1 b_2 - a_2 b_1 = \pm 1.$$

Nous avons déjà montré pour la base d'un corps que ce choix peut être fait d'une infinité de manières et qu'on obtient une nouvelle base. Le théorème est donc démontré.

Pour deux couples de nombres de base d'un idéal on peut faire valoir le théorème (p. 22) démontré pour les bases d'un corps.

Exemple. — Pour éclairer ce qui précède, nous allons traiter des exemples.

1[er] EXEMPLE $k(\sqrt{-5})$.

Dans ce corps on a

$$21 = 3.7 = (4 + \sqrt{-5})(4 - \sqrt{-5}) = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5})$$

formons les idéaux comme dans l'exemple des systèmes $4m + 1$

$$\begin{array}{ll} (3, 4 + \sqrt{-5}) & (3, 4 - \sqrt{-5}) \\ (3, 1 + 2\sqrt{-5}) & (3, 1 - 2\sqrt{-5}) \\ (7, 4 + \sqrt{-5}) & (7, 4 - \sqrt{-5}) \\ (7, 1 + 2\sqrt{-5}) & (7, 1 - 2\sqrt{-5}) \\ (4 + \sqrt{-5}, 1 + 2\sqrt{-5}) & (4 + \sqrt{-5}, 1 - 2\sqrt{-5}) \\ (4 - \sqrt{-5}, 1 + 2\sqrt{-5}) & (4 - \sqrt{-5}, 1 - 2\sqrt{-5}) \end{array}$$

Nous avons des idéaux par lesquels nous pourrons rendre unique la décomposition 3×7.

Les idéaux que nous venons d'énumérer ne sont pas tous différents l'un de l'autre, on se persuade facilement que

$$(3, 4 + \sqrt{-5}) = (3, 1 - 2\sqrt{-5})$$

car

$$\begin{aligned} 3.3 - 2(4 + \sqrt{-5}) &= 1 - 2\sqrt{-5} \\ (3, 4 + \sqrt{-5}) &= (3, 4 + \sqrt{-5}, 1 - 2\sqrt{-5}) \end{aligned}$$

de même

$$\begin{aligned} (3, 4 - \sqrt{-5}) &= (3, 1 + 2\sqrt{-5}) = (4 - \sqrt{-5}, 1 + 2\sqrt{-5}) \\ (7, 4 - \sqrt{-5}) &= (7, 1 + 2\sqrt{-5}) = (4 - \sqrt{-5}, 1 + 2\sqrt{-5}) \\ (7, 4 + \sqrt{-5}) &= (7, 1 - 2\sqrt{-5}) = (4 - \sqrt{-5}, 1 - 2\sqrt{-5}). \end{aligned}$$

En nous laissant guider par l'analogie avec notre système spécial nous écrirons

$$(21) = (3, 4 + \sqrt{-5})(3, 4 - \sqrt{-5})(7, 4 + \sqrt{-5})(7, 4 - \sqrt{-5})$$

et cette affirmation est exacte, car

$$\begin{aligned} (3) &= (3, 4 + \sqrt{-5})(3, 4 - \sqrt{-5}) \\ &= (9, 12 + 3\sqrt{5}, 12 - 3\sqrt{-5}, 21, 3) \end{aligned}$$

car comme

$$21 - 2.9 = 3$$

3 appartient aussi au produit d'idéaux et tous les nombres de cet idéal sont des multiples de 3, on voit de même que

$$(7,4 + \sqrt{-5})(7,4 - \sqrt{-5})$$
$$= (49,28 + 7\sqrt{-5}, 28 - 7\sqrt{-5}, 21) = (7).$$

Les idéaux

$$(3,4 + \sqrt{-5})(3,4 - \sqrt{-5})$$

mis sous la forme canonique, donnent

$$(3,1 + \sqrt{-5})(3,1 - \sqrt{-5})$$

comme on le voit aisément. L'idéal

$$(4 + \sqrt{-5}, 1 - 2\sqrt{-5})$$

n'est pas sous forme canonique, cherchons cette forme

$$(4 + \sqrt{-5}, 1 + 2\sqrt{5}) = (4 + \sqrt{-5}, 1 + 2\sqrt{-5}, 21, 7 \ldots)$$

Le plus commun diviseur les coefficients de $\sqrt{-5}$ est 1, nous pouvons poser

$$i_2 = 4 + \sqrt{-5}$$

le plus grand commun diviseur des nombres rationnels est $i_1 = 7$ nous avons donc la représentation canonique

$$(4 + \sqrt{-5}, 1 - 2\sqrt{-5}) = (7, 4 - \sqrt{-5})$$

Si nous faisons le produit de

$$(3,4 + \sqrt{-5})(7,4 + \sqrt{5})$$
$$(3,4 - \sqrt{-5})(7,4 + \sqrt{5})$$

on obtient deux idéaux

$$(21,28 - 7\sqrt{-5}, 12 - 3\sqrt{-5})$$
$$(21,28 - 7\sqrt{-5}, 12 + 3\sqrt{-5})$$

et on reconnaît que les représentations canoniques sont

$$(21, 10 + \sqrt{-5}), \qquad (21, 10 - \sqrt{-5}),$$

ces idéaux sont des idéaux principaux égaux comme on le montre facilement à

$$(1 - 2\sqrt{-5}), \qquad (1 + 2\sqrt{-5}).$$

L'idéal (2) dans le corps $k(\sqrt{-5})$ est le produit de deux idéaux non principaux

$$\begin{aligned}(2) &= (2, 1 + \sqrt{-5})(2, 1 - \sqrt{-5}) \\ &= (4, 2 + 2\sqrt{-5}, 2 - 2\sqrt{-5}, 6, 2 \ldots);\end{aligned}$$

mais comme

$$(2, 1 + \sqrt{-5}) = (2, 1 + \sqrt{-5}, 2 - 1 - \sqrt{-5})$$

on peut écrire aussi

$$(2) = (2, 1 + \sqrt{-5})^2.$$

2[e] Exemple : $k(\sqrt{10})$.

On a vu que

$$6 = 2.3 = (4 + \sqrt{10})(4 - \sqrt{10})$$

d'où l'on déduit

$$\begin{aligned}(2, 4 + \sqrt{10}) &= (2, \sqrt{10}) = (2, 4 - \sqrt{10}) \\ (3, 4 + \sqrt{10}) &= (3, 1 + \sqrt{10}) \\ (3, 4 - \sqrt{10}) &= (3, 1 - \sqrt{10})\end{aligned}$$

et tous ces idéaux sout sont forme canonique, et les deux décompositions différentes en donnant une seule

$$(6) = (2, \sqrt{10})^2 (3, 1 + \sqrt{10})(3, 1 - \sqrt{10}).$$

On voit d'ailleurs directement que

$$\begin{aligned}(2, \sqrt{10})^2 &= (4, 2\sqrt{10}, 10) = (2) \\ (3, 1 + \sqrt{10})(3, 1 - \sqrt{10}) &= (9, 3 + 3\sqrt{10}, 3 - 3\sqrt{10}, 6) = (3).\end{aligned}$$

D'une façon semblable on trouve

$$(5) = (5, \sqrt{10})(5, \sqrt{10})$$
$$(13) = (13, 6 + \sqrt{10})(13, 6 - \sqrt{10}).$$

3e Exemple : $k(\sqrt{-15})$.

Pour ce corps

$$m = -15 \equiv 1 \ (4)$$

les nombres entiers sont de la forme

$$a + b\,\frac{1 + \sqrt{-15}}{2} = a + b\omega$$

on vérifie facilement les décompositions suivantes :

$$(2) = (2, \omega)(2, \omega)$$
$$(3) = (3, \sqrt{-15})^2 = (3, -1 + 2\omega)^2$$
$$(5) = (5, \sqrt{-15})^2 = (5, -1 + 2\omega)^2$$
$$(17) = (17, 5 + \omega)(17, 5 + \omega')$$

et d'autres. Parmi ceux-là $(3, \sqrt{-15})$ $(5, \sqrt{-15})$ ne sont évidemment pas sous la forme canonique, mais on a

$$(3, \sqrt{-15}) = ((3, -1 + 2\omega, 3\omega - (-1 + 2\omega)) = (3, 1 + \omega)$$
$$(5, \sqrt{-15}) = (5, -1 + 2\omega, 5\omega - 2(-1 + 2\omega)) = (5, 2 = \omega).$$

10. Les corps dont tous les idéaux sont des idéaux principaux. — Lorsque dans un corps on peut appliquer l'algorithme d'Euclide pour la recherche du plus grand commun diviseur on peut énoncer le théorème suivant.

Théorème. — Soit un corps quadratique auquel on peut appliquer l'algorithme d'Euclide, les nombres de ce corps ne peuvent être décomposés en facteurs que d'une seule manière, et tous les idéaux du corps sont des idéaux principaux.

Démonstration. — Soit $k(\sqrt{m})$ le corps considéré et soit

$$\mathfrak{a} = (\alpha, \beta, \gamma \ldots) \text{ un idéal de ce corps}$$

ce théorème dit que l'idéal $\mathfrak{a}$ contient aussi le plus grand commun

diviseur de tous les nombres α, β, γ... que l'on obtient par la répétition de l'algorithme d'Euclide. Nous démontrerons tout d'abord que si α n'est pas divisible par β, mais que si ρ_n est le plus grand commun diviseur de α et de β, ρ_n appartient ainsi à l'idéal. Pour cela nous écrirons l'algorithme sous la forme

$$\begin{array}{llll} \alpha - \varkappa\beta - \rho_0 & & & = 0 \\ \quad \beta - \varkappa_1\rho_0 - \rho_1 & & & = 0 \\ \qquad \rho_0 - \varkappa_1\rho_1 - \rho_2 & & & = 0 \\ \ldots\ldots\ldots\ldots & & & \ldots \\ -\rho_n & & \rho_{n2} - \varkappa\rho_{n-1} & = 0. \end{array}$$

les $n+1$ équations peuvent être considérées comme un système d'équations linéaires à n inconnues $\rho_0\, \rho_1 \ldots \rho_{n-1}$, d'où il résulte par élimination

$$0 = \begin{vmatrix} \alpha - \varkappa\beta & -1 & 0 & 0 & \ldots & 0 \\ \beta & -\varkappa_1 & -1 & 0 & \ldots & 0 \\ 0 & 1 & -\varkappa_2 & -1 & \ldots & 0 \\ . & . & . & . & \ldots & 0 \\ 0 & . & 0 & 1 & -\varkappa_{n-1} \ldots & -1 \\ -\rho_n & & & & 1 & -\varkappa_n \end{vmatrix}.$$

Les $\varkappa$ sont tous des nombres entiers du corps, et par suite on a

$$\rho_n = \lambda_1\alpha + \lambda_2\beta.$$

Comme ici λ_1, λ_2 sont encore des entiers des corps ρ_n appartient à l'idéal. En répétant ce raisonnement il en résulte que A le plus grand commun diviseur de tous les nombres α, β, γ ... appartient à l'idéal c'est donc que

$$\mathfrak{a} = (A).$$

On peut dire que réciproquement que si tous les idéaux d'un corps sont des idéaux principaux, tous les nombres de ce corps ne peuvent être décomposés en facteurs que d'une seule manière.

11. Les congruences suivant les idéaux. — Nous écrivons

$$\alpha \equiv 0\ (\mathfrak{a})$$

et nous dirons que α est congru à 0 suivant le module $\mathfrak{a}$, quand α

et $\mathfrak{a}$ font partie du même corps et que α est un nombre de l'idéal $\mathfrak{a}$, de plus pour deux entiers du corps

$$\alpha \equiv \beta\ (\mathfrak{a})$$

α congru à β suivant le module $(\mathfrak{a})$ lorsque la différence $\alpha - \beta$ est contenu dans l'idéal $\mathfrak{a}$. Mais si α ou $\alpha - \beta$ n'appartient pas à l'idéal $\mathfrak{a}$ nous écrirons

$$\alpha \not\equiv 0\ (\mathfrak{a}) \quad \text{ou} \quad \alpha \not\equiv \beta\ (\mathfrak{a})$$

(nous dirons α est incongru à 0 ou incongru à β suivant le module $\mathfrak{a}$).

Remarque. — Nous introduisons tout d'abord cette définition d'une façon tout à fait formelle. Mais l'on voit immédiatement que cette définition coïncide pour celle des *congruences suivant des nombres*, lorsque $\mathfrak{a}$ est un idéal principal c'est-à-dire $\mathfrak{a} = (\alpha)$. Plus tard on montrera $\mathfrak{a}$ pour le cas où $\mathfrak{a}$ est un idéal quelconque que la définition coïncide essentiellement avec la définition antérieure de la congruence, car la congruence $\alpha \equiv 0\ (\mathfrak{a})$ signifie que l'idéal (α) est divisible par $\mathfrak{a}$.

Grâce à la définition d'un idéal et du produit $\mathfrak{a}$ de deux idéaux $\mathfrak{b}$ et $\mathfrak{c}$, nous pouvons nous exprimer de la manière suivante.

Si $\mathfrak{a}$ est un idéal divisible par l'idéal $\mathfrak{b}$, on a pour tous les nombres α, β, γ ... de $\mathfrak{a}$ les congruences

$$\alpha \equiv 0\ (\mathfrak{b}) \qquad \beta \equiv 0\ (\mathfrak{b})$$

Nous démontrerons plus loin la réciproque de ce théorème.

Etant donné un idéal $\mathfrak{a}$, on peut répartir tous les nombres du corps en classes, en attribuant tous les nombres congrus à un nombre donné suivant $\mathfrak{a}$ à une même classe. Alors deux nombres quelconques d'une même classe sont congrus mod $\mathfrak{a}$, et un nombre quelconque d'une classe détermine cette classe et ne détermine qu'elle. Autrement dit tout nombre entier appartient à une classe unique.

Chercher le nombre de ces classes, cela revient à chercher un système complet de nombres incongrus deux à deux suivant le module $\mathfrak{a}$, ou encore à chercher un système complet de restes suivant le module $\mathfrak{a}$.

Théorème. — Le nombre des nombres incongrus suivant un idéal

$$\mathfrak{a} = (i, i_1 + i_2\omega)$$

est

$$n(\mathfrak{a}) = i, i_2.$$

Démonstration : On a :

$$a + b\omega \not\equiv 0 \; (i, i_1 + i_2\omega)$$

pour toutes les combinaisons

$$a = 0, 1, 2 \ldots i - 1$$
$$b = 0, 1, 2 \ldots i_2 - 1$$

car tout nombre de l'idéal est de la forme

$$l_1 i + l_2 (i_1 + i_2\omega)$$

où l_1, l_2 sont des entiers rationnels. Ces (C combinaisons forment un système de ii_2 nombres dont deux quelconques ne peuvent être congrus suivant le module $\mathfrak{a}$. La différence de deux de ces nombres

$$a_k + b_k\omega - (a_{k'} + b_{k'}\omega)$$

n'est pas contenue dans l'idéal. Par contre tout nombre du corps est congru à *un* de ces nombres et à un seul.

En effet les nombres $a = 0 \ldots i - 1$, $b = 0 \ldots i_2 - 1$ forment des systèmes de restes complets, relativement à i et à i_2, on pourra faire correspondre à un nombre $A + B\omega$ du corps un nombre $a + b\omega$ choisi parmi ceux que nous venons de dire tel que l'égalité

$$(A + B\omega - (a + b\omega) = l_1 i + l_2 (i_1 + i_2\omega)$$

soit satisfaite pour deux valeurs rationnelles l_1 et l_2, car il faut choisir ab de telle sorte que

$$b \equiv B, (i_2) \quad \text{c'est-à-dire} \quad B - b = l_2 i_2$$

et

$$a \equiv A - l_2 i_1, (i)$$

$n(\mathfrak{a})$ a donc une signification particulière, nous dirons que $n(\mathfrak{a}$

est *la norme de l'idéal* $\mathfrak{a}$. Montrons qu'elle est indépendante de la base. Soit $\iota_1^* \iota_2^*$ une base quelconque de $\mathfrak{a}$, et soit

$$\iota_1^* = a_1 + b_1\omega \qquad \iota_2^* = a_2 + b_2\omega$$

nous pourrons trouver quatre entiers rationnels r, s, t, u, tels que

$$ru - ts = \pm 1$$

et que

$$\iota_1^* = ri + s(i_1 + i_2\omega), \qquad \iota_2^* = ti + u(i_1 + i_2\omega)$$

et il en résulte d'après le théorème relatif à la multiplication des déterminants

$$n(\mathfrak{a}) = \pm (a_1b_2 - a_2b_1) = ii_2.$$

La norme du produit de deux idéaux est égale au produit des normes. On peut démontrer cette proposition en considérant la définition de la norme qui vient d'être donnée. Nous en parlerons dans le chapitre relatif aux idéaux du corps cubique. Mais ici nous allons nous appuyer sur une autre définition de la norme.

12. La norme d'un idéal considérée comme produit d'idéaux. — Si l'on remplace tous les nombres $\alpha\ \beta\ \gamma$ ... d'un idéal, par leurs conjugués $\alpha'\ \beta'\ \gamma'$ ... ce qui revient au même si dans les nombres considérés on remplace ω par ω' on obtient un nouvel idéal $\mathfrak{a}'$, et $\mathfrak{a}$ est dit l'idéal conjugué de $\mathfrak{a}$. Nous le désignerons toujours par $\mathfrak{a}'$, ou $s(\mathfrak{a})$ lorsque nous ferons la substitution

$$s(\sqrt{m}) = -\sqrt{m}).$$

Nous dirons qu'un idéal qui coïncide avec son conjugué est un idéal ambige, c'est-à-dire si $\mathfrak{a} = \mathfrak{a}'$, il faudra de plus qu'il ne soit pas divisible par aucun nombre rationnel (idéal principal rationnel) autre que ± 1.

Théorème. — Le produit d'un idéal et de son conjugué est un idéal principal rationnel et l'on a

$$\mathfrak{a} \cdot \mathfrak{a}' = (n(\mathfrak{a})).$$

Démonstration [1] : Soit

$$\mathfrak{a} = (i, i_1 + i_2\omega) \quad \mathfrak{a}' = (i, i_1 + i_2\omega')$$

on sait que i et i_1 sont des multiples de i_2, on peut poser $i = ai_2$, $i_1 = a_1 i_2$, on a donc

$$\mathfrak{a} = (ai_2, a_1 i_2 + i_2\omega) = (i_2)(a, a_1 + \omega)$$

et de même

$$\mathfrak{a}' = \qquad\qquad = (i_2)(a, a_1 + \omega')$$

de plus on a la relation

$$(a_1 + \omega)(a_1 + \omega') \equiv 0 \ (a)$$

car a est le plus grand commun diviseur des nombres rationnels dans les idéaux $(a, a_1 + \omega)$ $(a, a_1 + \omega')$. Mais la multiplication des deux idéaux nous donne

$$\begin{aligned}\mathfrak{a} \cdot \mathfrak{a}' &= (i_2)(a, a_1 + \omega)(i_2)(a, a_1 + \omega') \\ &= (i_2^2)(a^2, aa_1 + a\omega, aa_1 + a\omega', (a_1 + \omega)(a_1 + \omega'))\end{aligned}$$

et il reste à démontrer que le deuxième facteur de ce produit est un idéal principal rationnel (a). Nous distinguerons pour cela trois cas de corps $k\sqrt{m}$.

1er *Cas.* — $m \equiv 3 \ (4)$, $\omega = \sqrt{m}$, $\omega' = -\sqrt{m}$.

On a alors

$$\begin{aligned}&(a^2, aa_1 + a\omega, aa_1 + a\omega', (a_1 + \omega)(a_1 + \omega')) \\ &= (a^2, aa_1 + a\sqrt{m}, aa_1 - a\sqrt{m}, a_1^2 - m) \\ &= (a^2, 2aa_1, 2a\sqrt{m}, 2am, a_1^2 - m) \\ &= (a)\left(a, 2m, \frac{a_1^2 - m}{a}, 2a_1, 2\sqrt{m}\right).\end{aligned}$$

Mais les nombres a, $2m$ et $\frac{a_1^2 - m}{a}$ ne peuvent avoir aucun facteur commun. Supposons d'abord que $q > 2$ divise a et m, on a

$$a_1^2 - m \equiv 0 \ (q) \qquad \text{car} \qquad a_1^2 - m \equiv 0 \ (a)$$

[1] Cette démonstration a été donnée par M. Hilbert dans son cours 1897-98.

et comme

$$m \equiv 0\ (q), \quad \text{on a} \quad a_1 \equiv 0\ (q).$$

Mais m ne contient aucun facteur au carré, a_1^2 est divisible par q^2, on a donc

$$a_1^2 - m = q\left(\frac{a_1^2}{q} - \frac{m}{q}\right)$$

$a_1^2 - m$ ne peut pas contenir q à une puissance supérieure à 1

$$\frac{a_1^2 - m}{a} \not\equiv 0\ (q).$$

Soit a divisible par $q = 2$, 2 divise a et $2m$ et comme

$$a_1^2 - m \equiv 0\ (a)$$

a_1 doit être impair

$$a^1 - m = -2, (4)$$

et $\frac{a_1^2 - m}{a}$ est impair et premier avec 2, les trois nombres a $2m$ $\frac{a_1^2 - m}{a}$ n'ont pas de diviseur commun et l'on peut choisir trois nombres l_1, l_2, l_3 tels que

$$l_1 a + l_2\, 2m + l_3 \frac{a_1^2 - m}{a} = 1.$$

Il en résulte

$$(a, a_1 + \omega)(a, a_1 + \omega') = (a)$$

et par suite

$$\mathfrak{a} \cdot \mathfrak{a}' = (i_2^2)(a) = (a i_2^2) = (i i_2)$$

ou comme nous l'avions affirmé $\mathfrak{a}\mathfrak{a}' = n\,(\mathfrak{a})$.

2° *Cas.* — $m \equiv 2\ (4)$, $\omega = \sqrt{m}$, $\omega' = -\sqrt{m}$.

Alors comme dans le premier cas

$$(a, a_1 + \omega)(a, a_1 + \omega') = (a)\left(a, 2m, \frac{a_1^2 - m}{a}, 2a_1, 2\sqrt{m}\right)$$

et les trois nombres a, $2m$ $\frac{a_1^2 - 2m}{a}$ ne peuvent avoir aucun facteur

commun $q > 2$. Mais ils ne peuvent avoir tous trois le facteur commun $q = 2$. En effet $a_1^2 - m \equiv 0 \ (a)$ nous montre que a_1 est plus pair et on a $a_1^2 - m \equiv -2 \ (4)$ c'est-à-dire que $\frac{a_1^2 - m}{a} \not\equiv 0 \ (2)$. Les trois nombres a, $2m$, $\frac{a_1^2 - m}{a}$ peuvent être composés de façon à donner 1 et on a comme dans le premier cas

$$(a, a_1 + \omega)(a, a_1 + \omega') = (a)$$

et

$$\mathfrak{a}\mathfrak{a}' = (ai_2^2) = n\,(a).$$

3ᵉ *Cas.* — $m \equiv 1 \ (4)$, $\omega = \frac{1 + \sqrt{m}}{2}$, $\omega' = \frac{1 - \sqrt{m}}{2}$.

Alors

$$(a, a_1 + \omega)(a, a_1 + \omega') = \left(a^2, 2aa_1 + a, a\sqrt{m}, \left(a_1 + \frac{1}{2}\right)^2 - \frac{m}{4}\right)$$

$$= (a)\left(a, m, \frac{\left(a_1 + \frac{1}{2}\right)^2 - \frac{m}{4}}{a}, 2a_1 + 1, \sqrt{m}\right)$$

le quatrième nombre $2a_1 + 1$ est impair, donc les quatre premiers nombres ne peuvent avoir le facteur commun 2. Si a et m sont divisibles par q,

$$\frac{\left(a_1 + \frac{1}{2}\right)^2 - \frac{m}{4}}{a}$$

est certainement premier avec q car $\left(a_1 + \frac{1}{2}\right)^2$ contient ce facteur deux fois, $\frac{m}{4}$ ne le contient qu'une fois. On peut conclure comme précédemment

$$\mathfrak{a}\mathfrak{a}' = (i_2^2)(a) = (ai_2^2) = (ii_2)$$

Le nombre $n(\mathfrak{a}) = ii_2$ est parmi les nombres de l'idéal $\mathfrak{a}$ et aussi dans ceux de $\mathfrak{a}'$. Si l'idéal $\mathfrak{a}$ n'est pas donné par la représentation canonique, mais par une base

$$i_1^* = a_1 + b_1\omega, \quad i_2^* = a_2 + b_2\omega$$

on a comme il a été montré au numéro précédent

$$\mathfrak{a}\mathfrak{a}' = n(\mathfrak{a}) = \pm(a_1 b_2 - a_2 b_1).$$

Considérons un produit d'idéaux

$$\mathfrak{a}\mathfrak{b}\mathfrak{c} \ldots \mathfrak{f},$$

on a d'après ce qui précède

$$n(\mathfrak{a} \cdot \mathfrak{b} \cdot \mathfrak{c} \ldots \mathfrak{f}) = \mathfrak{a} \cdot \mathfrak{b} \cdot \mathfrak{c} \ldots \mathfrak{f} \cdot \mathfrak{a}' \mathfrak{b}' \ldots \mathfrak{f}' = \mathfrak{a}\mathfrak{a}' \cdot \mathfrak{b}\mathfrak{b}' \ldots \mathfrak{f}\mathfrak{f}'$$
$$= n(\mathfrak{a})\, n(\mathfrak{b}) \ldots n(\mathfrak{f}).$$

Théorème. — Le système complet des restes suivant un nombre entier α du corps contient $|\, n(\alpha) \,|$ nombres.

Démonstration. — Le nombre que nous cherchons est égal à celui de nombres d'un système complet de restes suivant l'idéal principal $(\alpha) = \mathfrak{a}$. Nous choisirons comme base de l'idéal

$$\iota_1 = \alpha \qquad \iota_2 = \alpha\omega$$

posons

$$\alpha = a + b\omega.$$

On a dans le cas 1. $m \equiv 1 \ (4)$

$$\iota_1 = a + b\omega$$

$$\iota_2 = b\,\frac{m-1}{4} + (a+b)\,\omega$$

et par suite

$$n(\mathfrak{a}) = \left| a^2 + ab - \frac{m-1}{4}\, b^2 \right| = |\, n(\alpha) \,|.$$

2. pour le cas $m \not\equiv 1 \ (4)$

$$\iota_1 = a + b\omega$$
$$\iota_2 = bm + a\omega$$

et encore

$$n(\mathfrak{a}) = |\, a^2 - b^2 m \,| = |\, n(\alpha) \,|.$$

Exemple I. — Soit $\alpha = x + y\sqrt{-1}$ un nombre du corps

$$k(\sqrt{-1}) \qquad n(\alpha) = x^2 + y^2.$$

Dans ce corps la décomposition en facteurs n'est possible que d'une seule manière, tous les idéaux sont des idéaux principaux. Si donc $\pi = x + y\sqrt{-1}$ est un nombre irrationnel premier $n(\pi) = \pi \cdot \pi'$ est un nombre rationnel premier p, ce qu'on peut affirmer car p est rationnel. Le système complet des restes suivant ce nombre premier π contient p nombres du corps. Par contre soit q un entier rationnel indécomposable dans le corps, on a

$$n(q) = q^2.$$

Soit par exemple

$$5 = (2 + \sqrt{-1})(2 - \sqrt{-1})$$

les cinq nombres $0, 1, 2, \sqrt{-1}, 1 + \sqrt{-1}$ forment un système de reste complet suivant $\alpha = 2 + \sqrt{-1}$ [1]. Tout autre nombre du corps est congru à l'un de ces nombres suivant le module α par exemple.

$$-\sqrt{-1} \equiv 2\ (\alpha) \qquad -2 \equiv \sqrt{-1}\ (\alpha) \qquad -1 \equiv 1 + \sqrt{-1}\ (\alpha)$$
$$3 \equiv \sqrt{-1}\ (\alpha) \qquad 4 \equiv 1 + \sqrt{-1}\ (\alpha); \quad \text{etc., etc.}$$

De même les 9 nombres $0, \sqrt{-1}, 2\sqrt{-1}, 1, 1 + \sqrt{-1}, 1 + 2\sqrt{-1}, 2, 2 + \sqrt{-1}, 2 + 2\sqrt{-1}$ représentent un système complet de restes [2] suivant 3, car 3 est indécomposable dans le corps $k\sqrt{-1}$.

II. — Dans le corps $k(\sqrt{-5})$ on a, par exemple

$$3 = (3, 1 + \sqrt{5})(3, 1 - \sqrt{5})$$

et les trois nombres 0, 1, 2 forment un système complet de restes suivant le module $\mathfrak{p} = (3, 1 + \sqrt{5})$ ou $\mathfrak{p}' = (3, 1 - \sqrt{5})$; de plus $\mathfrak{p} = (11)$ est un nombre premier du second degré du corps et les 121 nombres $a + b\sqrt{-5}$ obtenus pour toutes les combinaisons $a = 0, 1 \ldots 10$, $b = 0, 1, 2 \ldots 10$ forment un système complet de restes suivant $\mathfrak{p} = (11, 11\sqrt{-5})$.

Nous allons établir maintenant un théorème important :

---

[1] Au lieu de ce système de nombres que l'on comprend sans explication, on pourrait le système des restes minima en valeur absolue $0, \pm 1, \pm\sqrt{-1}$.

[2] Le système des restes minima serait $0, \pm 1, \pm\sqrt{-1}, \pm 1 \pm \sqrt{-1}$.

Théorème. — Un idéal n'est divisible que par un nombre fini d'idéaux.

Démonstration : Soit $\mathfrak{j} = \mathfrak{a}, \mathfrak{b}, \mathfrak{c} \ldots$, on a

$$n(\mathfrak{j}) = n(\mathfrak{a})\, n(\mathfrak{b})\, n(\mathfrak{c}) \ldots$$

Mais $n(\mathfrak{j})$ est un nombre entier rationnel et ne peut être divisible que par un nombre limité d'entiers rationnels > 1, le nombre des idéaux $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$, ... sera donc fini. Il est entendu qu'on excepte les idéaux égaux à l'unité.

En combinant les trois derniers théorèmes, on obtient finalement le résultat.

Théorème. — Il n'y a qu'un nombre fini d'idéaux dont la norme est inférieure à un nombre donné.

On peut donner une autre forme à l'énoncé de ce théorème et dire :

Il n'y a qu'un nombre fini d'idéaux différents qui contiennent tous un nombre fini donné α.

Lorsqu'un idéal divise un nombre premier p, p est un nombre de l'idéal, et dans la représentation canonique

$$(i,\ i_1 + i_2\omega)$$

il faut $i = p$, $i = 1$ donnerait un idéal unité, quant à i_2 qui doit être un diviseur de $i = p$, il peut se présenter deux cas ou $i_2 = 1$, $i_1 < p$ ou $i_2 = p$ et alors i_1 qui doit être alors un multiple de p, peut être pris $= 0$. On a donc les deux cas

$$(p,\ i_1 + \omega) \quad \text{et} \quad (p,\ p\omega)$$

dont les normes sont p ou p^2, d'où le

Théorème. — La norme d'un idéal qui divise un nombre premier rationnel p, est p ou p^2.

Dans le premier cas l'idéal est dit du premier degré, dans l'autre il est dit du second degré.

1er Exemple : $k(\sqrt{-5})$.

1. $\mathfrak{j} = (2,\ 1 + \sqrt{-5})$ $\quad \mathfrak{j}' = (2,\ 1 - \sqrt{5})$

alors d'après le théorème général $n(j) = 2$ et

$$\mathfrak{j}\mathfrak{j}' = (4,\ 2 + 2\sqrt{-5},\ 2 - 2\sqrt{-5},\ 6,\ 2) = (2)$$

2. $\mathfrak{j} = (3,\ 1 + \sqrt{-5})$ $\quad \mathfrak{j}' = (3,\ 1 - \sqrt{-5})$

$n(\mathfrak{j}) = 3$ et $\mathfrak{j}\mathfrak{j}' = (9,\ 3 + 3\sqrt{-5},\ 3 - 3\sqrt{-5},\ 6,\ 3) = (3)$

3. $\mathfrak{j} = (4 + \sqrt{-5},\ 1 + 2\sqrt{-5})$ $\quad \mathfrak{j}' = (4 - \sqrt{-5},\ 1 - 2\sqrt{-5})$

$n(\mathfrak{j}) = 7$ et $\mathfrak{j}\mathfrak{j}' = (21,\ 14 + 7\sqrt{-5},\ 14 - 7\sqrt{-5},\ 28,\ 7) = (7)$

4. $\mathfrak{j} = (4 - \sqrt{-5},\ 1 + 2\sqrt{-5})$ $\quad \mathfrak{j}' = (4 + \sqrt{-5},\ 1 - 2\sqrt{-5})$

$$\mathfrak{j}\mathfrak{j}' = (21,\ -6 + 9\sqrt{-5},\ -6 - 9\sqrt{-5},\ -12,\ 3) = (3)$$

et par suite $n(\mathfrak{j}) = 3$ et en effet on voit facilement que cet exemple est identique à l'exemple 2

5. $\mathfrak{j} = (21,\ 10 + \sqrt{-5})$ $\quad \mathfrak{j}' = (21,\ 10 - \sqrt{-5})$

$n(\mathfrak{j}) = 21$ $\quad \mathfrak{j}\mathfrak{j}' = (441,\ 210 + 21\sqrt{-5},\ 210 - 21\sqrt{-5},\ 105) = (21)$

2° Exemple : $k(\sqrt{-15})$.

1. $\mathfrak{j} = (2, \omega) = \left(2,\ \dfrac{1 - \sqrt{-15}}{2}\right)$ $\quad \mathfrak{j}' = \left(2,\ \dfrac{1 - \sqrt{-15}}{2}\right)$

$n(\mathfrak{j}) = 2$, $\mathfrak{j}\mathfrak{j}' = (4,\ 1 + \sqrt{-15},\ 1 - \sqrt{-15},\ 2) = (4,\ 2\omega,\ 2\omega',\ 2) = (2)$

2. $\mathfrak{j} = (3,\ \sqrt{-15})$ $\quad \mathfrak{j}' = (3,\ -\sqrt{-15}) = (3,\ 1 + \omega)$

$n(\mathfrak{j}) = 3$ et $\mathfrak{j}\mathfrak{j}' = (9,\ 3\sqrt{-15},\ 15,\ 3) = (3)$

3. $\mathfrak{j} = (17,\ 5 + \omega)$ $\quad \mathfrak{j}' = (17,\ 5 + \omega')$

$n(\mathfrak{j}) = 17$ et $\mathfrak{j}\mathfrak{j}' = (289,\ 85 + 17\omega,\ 85 + 17\omega',\ 34) = (17)$

4. $\mathfrak{j} = (93,\ 13 + \omega)$ $\quad n(\mathfrak{j}) = 93$

$$\mathfrak{j}\mathfrak{j}' = (93^2,\ 13 \cdot 93 + 93 \cdot \omega,\ 13 \cdot 93 + 93 \cdot \omega',\ 186,\ 93) = (93).$$

Le lecteur formera lui-même les systèmes de restes complets suivant les idéaux précédents.

13. La décomposition en facteurs idéaux n'est possible que d'une seule manière. *Théorème.* — Soit $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ trois idéaux différents de zéro, si l'on a

$$\mathfrak{a}\mathfrak{b} = \mathfrak{a}\mathfrak{c}$$

on a $\mathfrak{b} = \mathfrak{c}$.

Démonstration : de l'hypothèse il résulte

$$\mathfrak{a}'\mathfrak{a}\mathfrak{b} = \mathfrak{a}'\mathfrak{a}\mathfrak{c}$$
$$n(\mathfrak{a})\,\mathfrak{b} = n(\mathfrak{a})\,\mathfrak{c}$$

et comme on peut diviser par le facteur numérique $n(\mathfrak{a})$

$$\mathfrak{b} = \mathfrak{c}.$$

Théorème. — Si tous les nombres d'un idéal $\mathfrak{a}$ sont congrus à zéro suivant un idéal $\mathfrak{b}$, on en conclut que $\mathfrak{a}$ est divisible par $\mathfrak{b}$.

Démonstration : Soient les idéaux

$$\mathfrak{a} = (\alpha_1 \alpha_2 \ldots) \quad \text{et} \quad \mathfrak{b} = (\beta_1, \beta_2 \ldots)$$

on a par hypothèse

$$\alpha_1 \equiv 0\ (\mathfrak{b})$$
$$\alpha_2 \equiv 0\ (\mathfrak{b}).$$

Multiplions $\mathfrak{a}$ et $\mathfrak{b}$ par $\mathfrak{b}'$ on a $\mathfrak{b}\mathfrak{b}' = (n(\mathfrak{b}))$; nous montrerons d'abord que $\mathfrak{a}\mathfrak{b}'$ est divisible par $\mathfrak{b}\mathfrak{b}'$. On a pour tous les nombres de $\mathfrak{a}\mathfrak{b}'$ la congruence

$$\alpha_1 \beta'_1 \equiv 0 \qquad \alpha_1 \beta'_2 \equiv 0 \ldots (\mathfrak{b}\mathfrak{b}')$$
$$\alpha_2 \beta'_1 \equiv 0 \qquad \alpha_2 \beta'_2 \equiv 0 \ldots (\mathfrak{b}\mathfrak{b}') \text{ et ainsi de suite}$$

mais comme $(\mathfrak{b}\mathfrak{b}') = (n(\mathfrak{b}))$ est un idéal principal rationnel, on peut poser

$$\alpha_1 \beta'_1 = n(\mathfrak{b})\,\gamma_{11} \qquad \alpha_1 \beta'_2 = n(\mathfrak{b})\,\gamma_{12} \ldots$$
$$\alpha_2 \beta'_1 = n(\mathfrak{b})\,\gamma_{21} \qquad \alpha_2 \beta'_2 = n(\mathfrak{b})\,\gamma_{12} \ldots \text{ et ainsi de suite}$$

où $\gamma_{11}\ \gamma_{12}$ sont des entiers du corps, et l'on voit immédiatement que

$$\mathfrak{a}\mathfrak{b}' = (n(\mathfrak{b}))\,(\gamma_{11}, \gamma_{12} \ldots)$$

$(\gamma_{11}\ \gamma_{12} \ldots) = \mathfrak{c}$ est un nouvel idéal qu'on obtient en divisant tous les nombres de l'idéal $\mathfrak{a}\mathfrak{b}'$ par le facteur commun $n(\mathfrak{b})$.

On a donc

$$\mathfrak{a}\mathfrak{b}' = \mathfrak{b}\mathfrak{b}'\mathfrak{c}$$

et par suite

$$\mathfrak{a} = \mathfrak{b}\mathfrak{c}$$

c'est ce que nous voulions démontrer.

Corollaire. — Le plus grand commun diviseur $\mathfrak{t}$ de deux idéaux $\mathfrak{a}$ et $\mathfrak{b}$ est un idéal qui contient à la fois tous les nombres de $\mathfrak{a}$ et tous ceux de $\mathfrak{b}$.

Soit

$$\mathfrak{a} = (\alpha_1, \alpha_2 \ldots) \qquad \mathfrak{b} = (\beta_1\ \beta_2 \ldots)$$
$$\mathfrak{t} = (\alpha_1, \alpha_2 \ldots \beta_1, \beta_2 \ldots).$$

En effet un idéal qui divise $\mathfrak{a}$ et $\mathfrak{b}$ doit contenir tous les nombres de $\mathfrak{a}$ et tous les nombres de $\mathfrak{b}$. Comme d'autre part tout idéal qui contient tous ces nombres et qui contient en outre d'autres nombres ne résultant pas de combinaisons linéaires des α et des β divise $\mathfrak{t}$, on peut dire que $\mathfrak{t}$ est le plus grand commun diviseur de $\mathfrak{a}$ et de $\mathfrak{b}$.

Théorème. — Si un idéal premier $\mathfrak{p}$ divise un produit de deux idéaux $\mathfrak{a}$ et $\mathfrak{b}$ et si $\mathfrak{p}$ ne divise pas $\mathfrak{b}$ il divise $\mathfrak{a}$ ou encore si un idéal premier $\mathfrak{p}$ divise un produit de deux idéaux $\mathfrak{ab}$ il divise au moins l'un des facteurs.

Démonstration : Soit

$$\mathfrak{p} = (\pi_1, \pi_2 \ldots)$$

comme $\mathfrak{p}$ ne divise pas $\mathfrak{b}$, il n'y a pas en dehors des idéaux unités d'autre idéal divisant à la fois $\mathfrak{b}$ et $\mathfrak{p}$

$$\mathfrak{t} = (\beta_1, \beta_2 \ldots \pi_1, \pi_2 \ldots)$$

est donc un idéal unité, et l'on peut déterminer un nombre β de $\mathfrak{b}$ et un nombre π de y tels que

$$\beta + \pi = 1.$$

Mais comme $\mathfrak{ab}$ est divisible par $\mathfrak{p}$ on a les congruences

$$\alpha_1\ \beta_1 \equiv 0,\ \alpha_1\ \beta_2 \equiv 0 \ldots (\mathfrak{p})$$
$$\alpha_1\ \beta_2 \equiv 0,\ \alpha_2\ \beta_2 \equiv 0 \ldots (\mathfrak{p})$$
$$\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot$$
$$\alpha_1\ \beta \equiv 0,\ \alpha_2\ \beta_2 \equiv 0 \ldots (\mathfrak{p})$$

d'ailleurs pour le nombre π on a $\pi \equiv 0\ (\mathfrak{p})$ par suite on a aussi

$$\alpha_1\ (\beta + \pi) = 0, \qquad \alpha_2\ (\beta + \pi) = 0 \ldots (\mathfrak{p})$$

et comme $\beta + \pi = 1$ on a

$$\alpha_1 \equiv 0 \quad \alpha_2 \equiv 0 \quad \alpha_3 \equiv 0 \ldots (\mathfrak{p})$$

donc $\mathfrak{a}$ est divisible par $\mathfrak{p}$.

Nous démontrerons facilement le théorème fondamentale

Théorème fondamental. — Tout idéal ne peut être décomposé en un produit d'idéaux premiers que d'une seule manière.

Démonstration : Soit $\mathfrak{j}$ l'idéal considéré et soit

$$\mathfrak{j} = \mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_n$$

Admettons qu'une deuxième décomposition nous ait donné

$$\mathfrak{j} = \mathfrak{q}_1 \mathfrak{q}_2 \mathfrak{q}_3 \cdots \mathfrak{q}_n$$

on aurait

$$\mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_n = \mathfrak{q}_1 \mathfrak{q}_2 \cdots \mathfrak{q}_n$$

$\mathfrak{q}_1$ doit diviser le premier membre, il divise $\mathfrak{p}$ et alors il est égal à $\mathfrak{p}$, ou il divise le produit $\mathfrak{p}_1 \ldots \mathfrak{p}_n$. Dans ce dernier cas il faudrait avoir $\mathfrak{q}_1 = \mathfrak{p}_2$ ou $\mathfrak{q}_1$ diviserait le produit $\mathfrak{p}_3 \ldots \mathfrak{p}_n$ et ainsi de suite tout facteur de l'un des produits doit être contenu dans l'autre ce qui démontre le théorème.

En somme cet démonstration est fondée sur ce fait que $n(\mathfrak{a}) = \mathfrak{a}.\mathfrak{a}'$ autrement dit sur ce fait qu'étant donné un idéal $\mathfrak{a}$ on peut toujours lui adjoindre un idéal $\mathfrak{a}'$ tel que $\mathfrak{a}\mathfrak{a}'$ devienne un idéal principal rationnel. Ce théorème s'énonce sous une forme plus générale dans la théorie du corps algébrique. A tout idéal $\mathfrak{a}$ on peut adjoindre un idéal $\mathfrak{a}_1$ tel que le produit $\mathfrak{a}\mathfrak{a}_1$ soit un idéal principal et ce théorème sur lequel on s'appuie pour démontrer le théorème fondamental dans la théorie générale. Les démonstrations plus anciennes dues à Dedekind (Suppl. XI) et à Kronecker étaient beaucoup plus compliquées. M. Hurwitz parvint à les simplifier beaucoup grâce à un théorème de Monsieur Kronecker [1] sur les diviseurs d'un système de nombres entiers.

---

(1) Pour être complet il nous faut citer ce théorème ici le lecteur en comprendra mieux l'énoncé après avoir vu le 4e chapitre.

Théorème. Lorsque les coefficients $\alpha_0, \alpha_1 \ldots \beta_0, \beta_1$ des fonctions de n

$$\varphi(x) = \alpha_0 x^r + \ldots \alpha$$
$$\psi(x) = \beta_0 x^s + \ldots \beta,$$

Nous donnerons plus loin une deuxième démonstration due à Monsieur Hurwitz [1] [2].

M. Hilbert a donné une démonstration simple qui ne s'appuie pas sur le théorème de Kronecker et fondée sur la notion du corps de Galois [3]. Le théorème ne peut être encore utilisé pratiquement car on manque de méthode facile pour reconnaître si un idéal est premier, et pour trouver les facteurs d'un idéal qui n'est pas premier.

Le théorème suivant fournit en partie la solution théorique de ces problèmes.

Théorème. — Tout idéal premier $\mathfrak{p}$ du corps $k(\sqrt{m})$ divise un nombre premier rationnel p au plus exactement il divise toujours un idéal principal rationnel (p).

Soit $\mathfrak{p}$ un idéal premier $n(\mathfrak{p}) = \mathfrak{p}.\mathfrak{p}'$ est un idéal principal rationnel. Décomposons $n(\mathfrak{p})$ en ses facteurs premiers $pq \dots r$ comme $\mathfrak{p}\mathfrak{p}'$ divise $n(\mathfrak{p})$ divise aussi $n(\mathfrak{p})$ et par suite l'un des facteurs (p) ou $(q \dots r)$ s'il divise p le théorème est démontré sinon il divise $(q \dots r)$ etc. etc., c'est-à-dire que $(\mathfrak{p})$ divise un nombre premier désignons le par p. $\mathfrak{p}$ ne peut diviser un second nombre premier q sans quoi $\mathfrak{p}$ serait un idéal unité. De même $\mathfrak{p}$ divise p et ne divise pas un autre nombre premier. Un idéal tel que $\mathfrak{p}$ ne peut contenir que des nombres rationnels qui sont multiples de p et ne peut contenir que des nombres α du corps dont la norme $n(\alpha)$ est divisible par p.

Un idéal premier est dit du premier ou du second degré suivant que sa norme est égale à p ou à p^2. Pour avoir les facteurs premiers d'un idéal quelconque $\mathfrak{a}$, on forme $n(\mathfrak{a})$, on décompose ce nombre

---

sont des nombres algébriques entiers et lorsque les coefficients du produit des deux fonctions

$$\varphi(x)\,\psi(x) = \gamma_0 x^{r+s} + \dots + \gamma_{r+s}\,,$$

sont tous divisibles par un nombre algébrique ω chacun des $(r+1)(s+1)$ nombre $\alpha_i\beta_k$ est divisible par ω. (Hurwitz Gött. Nach. 1894, p. 291-292).

(1) [Hurwitz, *Gött. Nachr.* 1894 p. 291-292]. Comparer *Kronecker*, Werke II, p. 47. M J. König a donné une démonstration simple du théorème général. Introduction à la théorie des grandeurs algébriques. Leipzig, 1903.

(2) *Nachr. der K. Ges. d. Wissensch. zu Göttingen. Math. phys. Klasse*. 1894.

(3) *Math. Annalen, Bd.* 44, *Année* 1894. *p.* 1 *Jahresber. d. Deutsch. Math. Vereinig.* t. 3 1894, p. 50.

rationnel en ses facteurs premiers, et enfin on décompose ceux-là en idéaux premiers.

On ne pourra pas indiquer une infinité de nombres pour déterminer un idéal, par exemple un idéal qui divise p. En fait un idéal principal est déterminé par un seul nombre, et un idéal non principal peut être déterminé par deux nombres, sans qu'il soit nécessaire que ces deux nombres forment une base de l'idéal.

On a d'ailleurs le théorème suivant.

Théorème. — Tout idéal $\mathfrak{j}$ peut être représenté par (α, β) comme p. g. c. d. des nombres entiers α et β.

Il suffit de choisir dans l'idéal deux nombres α et β qui sont d'ailleurs divisibles par $\mathfrak{j}$ et tels que $\frac{(\alpha)}{\mathfrak{j}}$ et $\frac{(\beta)}{\mathfrak{j}}$ soient premiers entre eux, on a alors $\mathfrak{j} = (\alpha, \beta)$.

14. Les diviseurs des nombres premiers rationnels dans le corps $k(\sqrt{m})$. — Un idéal premier $\mathfrak{p}$ divise toujours un nombre premier rationnel p nous avons montré qu'il a toujours l'une des formes

$$1.)\quad \mathfrak{p} = (p, a + \omega) \qquad \text{ou} \qquad 2.)\quad \mathfrak{p} = (p, p\omega).$$

Dans le premier cas $p = \mathfrak{p}\mathfrak{p}'$, c'est-à-dire que (p) peut être considéré en un produit de deux idéaux du premier degré, dans le second cas $\mathfrak{p} = (p)$, (p) ne se décompose pas, mais représente lui-même un idéal premier du second degré.

Nous allons établir un critère qui nous permettra de reconnaître si un nombre premier p du corps $k(\sqrt{m})$ se décompose au moyen d'un calcul très court.

1er *Cas*. — $m \equiv 3\ (4)$. Le discriminant du corps est $4m$.

Soit p un nombre premier qui ne divise pas le discriminant et en particulier soit $p \not\equiv 2$. Si p peut se décomposer on a

$$\mathfrak{p} = (p, a + \sqrt{m})$$

a doit satisfaire à la congruence

$$(a + \sqrt{m})(a - \sqrt{m}) = a^2 - m \equiv 0\ (p).$$

Réciproquement si la congruence

$$x^2 - m \equiv 0\ (p)$$

admet une solution entière rationnelle $x = a$, p peut être décomposé en un produit de deux idéaux du premier degré.

Car soit $x \equiv a$ une racine de la congruence $x^2 - m \equiv 0\ (p)$ et non de

$$x^2 - m \equiv 0\ (p^2), \quad \mathfrak{p} = (p, a + \sqrt{m}), \quad \mathfrak{p}' = (p, a - \sqrt{m})$$

seront deux idéaux facteurs de (p). Ces deux idéaux sont différents, car en tenant compte de ce que a est premier avec p, le plus grand commun diviseur de $\mathfrak{p}$ et de $\mathfrak{p}'$ c'est-à-dire

$$(p, a + \sqrt{m}, a - \sqrt{m}, 2a, 1)$$

est un idéal premier, ce qui n'est vrai ni de $\mathfrak{p}$ ni de $\mathfrak{p}'$. Enfin $\mathfrak{p}$ et $\mathfrak{p}'$ sont différents de (p) car p ne divise ni $a + \sqrt{m}$, ni $a - \sqrt{m}$ et l'on a $(p) = \mathfrak{p}\mathfrak{p}'$.

Pour écrire que la congruence $x^2 \equiv m \bmod p$. admet une solution a, telle que $a^2 \not\equiv m\ (p^2)$ nous emploierons le *symbole de Legendre*, nous écrirons $\left(\frac{m}{p}\right) = 1$.

Si l'on suppose $p > 2$ la congruence $x^2 - m \equiv 0\ (p)$ a toujours une solution lorsqu'il en est ainsi de

$$y^2 - 4m \equiv 0\ (p) \quad \text{ou} \quad y^2 - d \equiv 0\ (p).$$

Car parmi les solutions de cette dernière il y a des nombres pairs y et il suffit de poser $x = \frac{y}{2}$.

Au lieu d'écrire $\left(\frac{m}{p}\right) = 1$, nous écrirons donc $\left(\frac{d}{p}\right) = \pm 1$.

Si $x^2 - m = 0\ (p)$ ou ce qui revient au même si $y^2 - 4m \equiv 0\ (p)$ n'a pas de solution p ne se décompose pas dans le corps $k(\sqrt{m})$ et nous donne un idéal premier du second degré. C'est ce qu'on écrit

$$\left(\frac{m}{p}\right) = \left(\frac{4m}{p}\right) = \left(\frac{d}{p}\right) = -1.$$

Il nous reste à considérer les nombres premiers qui divisent le discriminant du corps, premièrement $p = 2$ et les facteurs premiers simples impairs de m.

La congruence

$$x^2 - m \equiv 0\ (2)$$

admet pour solutions $x = \pm 1$, ces deux solutions sont identiques mod. 2.

On a donc comme idéaux premiers facteurs de (2)

$$\mathfrak{p} = (2, 1 + \sqrt{m}) \qquad \mathfrak{p}' = (2, 1 - \sqrt{m})$$

le cas diffère cependant des autres en ce que les deux idéaux $\mathfrak{p}$ et $\mathfrak{p}'$ sont égaux.

$$(2, 1 + \sqrt{m}) = (2, 1 + \sqrt{m}, 1 - \sqrt{m}) = (2, 1 - \sqrt{m})$$

ou $\mathfrak{p} = \mathfrak{p}'$. Comme $\mathfrak{p}$ n'est pas un idéal unité et que 2 ne divise pas $1 + \sqrt{m}$, (2) est dans le corps $k\sqrt{m}$ le carré d'un idéal premier $= \mathfrak{p}^2$.

Enfin soit p un facteur premier impair de d (il n'y entre qu'au premier degré car m par hypothèse ne renferme pas de facteur carré), alors la congruence

$$x^2 - m \equiv 0 \ (p)$$

admet la solution $x = 0$ et p est divisible par

$$\mathfrak{p} = (p, \sqrt{m}) \qquad \text{et} \qquad \mathfrak{p}' = (p, -\sqrt{m})$$

ces deux idéaux $\mathfrak{p}$ et $\mathfrak{p}'$ sont évidemment identiques et différents de 1 et

$$\mathfrak{p} \cdot \mathfrak{p}' = \mathfrak{p}^2 = (p^2, p\sqrt{m}, m, p) = (p).$$

Donc tout facteur premier rationnel du discriminant du corps est divisible par le carré d'un idéal premier.

Nous généraliserons le symbole de Legendre et nous exprimerons que $y^2 - d \equiv 0 \ (p)$ n'a qu'une solution $y \equiv 0 \ (p)$ en écrivant $\left(\frac{d}{p}\right) \equiv 0$.

2e *Cas.* — $m = 2 \ (4)$ le discriminant $d = 4m$.

On raisonnera comme précédemment et on trouvera qu'un nombre premier qui ne divise pas d se décompose ou non suivant que

$$\left(\frac{d}{p}\right) = +1 \qquad \text{ou} \qquad \left(\frac{d}{p}\right) = -1.$$

De plus on a pour 2

$$(2) = (2, \sqrt{m})^2 = \mathfrak{p}^2$$

et pour tout nombre impair qui divise d, c'est-à-dire m

$$(p) = (p, \sqrt{m})^2 = \mathfrak{p}^2.$$

Dans ces deux cas la congruence $x^2 - d \equiv 0$ a la racine double $x = 0$, ce qu'on écrit encore $\left(\frac{d}{p}\right) = 0$.

3° *Cas.* — $m \equiv 1$ (4) le discriminant $d = m$.

Soit d'abord p un nombre premier impair qui ne divise pas m si p se décompose

$$\mathfrak{p} = (p, a + \omega)$$

et par suite

$$(a + \omega)(a + \omega') = \left(a + \frac{1}{2}\right)^2 - \frac{m}{4}$$

est divisible par p mais si

$$\left(a + \frac{1}{2}\right)^2 - \frac{m}{4}$$

est divisible par m il en est de même de

$$4\left[\left(a + \frac{1}{2}\right)^2 - \frac{m}{4}\right]$$

et réciproquement.

Il en résulte la condition *nécessaire* pour que p se décompose et que $x^2 - d \equiv 0$ (p) admettre une solution, c'est-à-dire $\left(\frac{d}{p}\right) + = 1$.

Réciproquement si $\left(\frac{d}{p}\right) = +1$, c'est-à-dire si $x^2 - d \equiv 0$ (p) admet des solutions, on peut toujours prendre parmi ces solutions de nombre impair $2a + 1$ et alors

$$\mathfrak{p} = (p, a + \omega) \qquad \mathfrak{p}' = (p, a + \omega')$$

sont deux idéaux premiers différents facteurs de p. Et en effet le plus grand commun diviseur de $\mathfrak{p}$ et de $\mathfrak{p}'$ est

$$(p, a + \omega, a + \omega', 2a + 1, 1) = (1)$$

car $2a+1$ est premier avec p. De plus $\mathfrak{p}$ ni $\mathfrak{p}'$ ne peut être égal à (1) ou à (p) car p ne divise ni $a+\omega$ ni $a+\omega'$.

Soit ensuite $p=2$.

Si (2) est divisible par $\mathfrak{p}=(2, a+\omega)$ il faut que

$$(a+\omega)(a+\omega') \equiv \left(a+\frac{1}{2}\right)^2 - \frac{m}{4}$$

soit pair, c'est-à-dire que $(2a+1)^2 - m$ soit divisible par 8 ou encore que la congruence $x^2 - m \equiv 0$ (8) admette une solution. Réciproquement si cette congruence admet des solutions, ce ne peuvent être que des nombres impairs et si $2a+1$ est une de ces solutions,

$$\mathfrak{p}=(2, a+\omega) \quad \mathfrak{p}'=(2, a+\omega')$$

seront deux idéaux différents premiers qui divisent (2) $\mathfrak{p}$ et $\mathfrak{p}'$ sont différents car leur plus grand commun diviseur est

$$(2, a+\omega, a+\omega', 2a+1, 1) = (1).$$

Faisons l'hypothèse essentielle $d \equiv 1$ (2) et posons $\left(\frac{d}{2}\right) = +1$ ou -1 suivant que $x^2 - d \equiv 0$ (8) admet une solution ou non.

$p=2$ se décompose dans le corps K $(\sqrt{m})$ suivant que

$$\left(\frac{d}{2}\right) = +1 \quad \text{ou} \quad \left(\frac{d}{2}\right) = -1.$$

On voit d'ailleurs facilement que $\left(\frac{d}{2}\right) = +1$ pour $m \equiv 1$ (8) et $\left(\frac{d}{2}\right) = -1$ pour $m = 5$ (8).

Enfin soit p un nombre premier impair qui divise m, $x \equiv 0$ (p) est une racine double de la congruence $x^2 - d \equiv 0$ (p) et l'on pose $\left(\frac{d}{p}\right) = 0$.

$$\mathfrak{p}=(p, \sqrt{m}) \quad \mathfrak{p}'=(p, -\sqrt{m})$$

sont des idéaux premiers qui divisent p, et comme $\mathfrak{p}=\mathfrak{p}'$ on a

$$(p) = \mathfrak{p}^2.$$

On peut prendre pour base

$$\omega_1 = p \qquad \omega_2 = \frac{p - 1}{2} + \omega.$$

On voit qu'ici encore les diviseurs du discriminant du corps sont les carrés d'un idéal premier.

En réunissant ces 3 cas on voit que :

Théorème. — Dans le corps $k(\sqrt{m})$ de discriminant d un nombre entier rationnel p est égal au produit de deux idéaux premiers conjugués mais différents, où est le carré d'un idéal premier, ou enfin ne peut se décomposer suivant que

$$\left(\frac{d}{p}\right) = + 1 \qquad \left(\frac{d}{p}\right) = 0 \qquad \text{ou} \qquad \left(\frac{d}{p}\right) = - 1.$$

Nous apprendrons plus loin à calculer le symbole $\left(\frac{d}{p}\right)$ comme application de la loi de réciprocité quadratique, mais il nous est possible de donner dès maintenant quelques exemples.

Corps

$$(K\sqrt{-5}) \qquad m = -5 \qquad d = -20$$

les nombres 2 et 5 sont les seuls facteurs premiers du discriminant, ces nombres doivent donc être divisibles par les carrés d'idéaux premiers. Et en effet

$$(2) = (2, 1 + \sqrt{-5})^2 \qquad (5) = (\sqrt{-5})^2.$$

La congruence $x^2 + 5 \equiv 0\ (p)$ admet des solutions pour $p = 3$, 7, 23 ... elle est impossible pour $p = 11$, 13, 17, 19 etc., on a donc les décompositions

$$(3) = (3, 1 + \sqrt{-5})(3, 1 - \sqrt{-5})$$
$$(7) = (7, 3 + \sqrt{-5})(7, 3 - \sqrt{-5})$$
$$(23) = (23, 8 + \sqrt{-5})(23, 8 - \sqrt{-5})$$

tandis que (11) (13) (17) (19) représentent des idéaux principaux du second degré.

Corps

$$K(\sqrt{35}) \qquad m = 35 \qquad d = 140.$$

---

(1) Hilbert. — *Zahlbericht*, 661, p. 284.

Les nombres premiers contenus dans le discriminant sont 2, 5, 7 et par suite

$$(2) = (2, 1 + \sqrt{35})^2$$
$$(5) = (5, \sqrt{35})^2$$
$$(7) = (7, \sqrt{35})^2$$

La congruence $x^2 - 35 = 0$ (p) admet des solutions pour $p = 13, 17, 19$ etc., elle est impossible pour $p = 3, 11$ etc., on a les décompositions

$$(13) = (13, 3 + \sqrt{35})\,(13, 3 - \sqrt{35})$$
$$(17) = (17, 1 + \sqrt{35})\,(17, 1 - \sqrt{35})$$
$$(19) = (19, 4 + \sqrt{35})\,(19, 4 - \sqrt{35})$$

(3) et (11) sont des idéaux premiers du second degré.

15. Le théorème fondamental des formes linéaires. — Nous allons exposer un théorème que nous appliquerons souvent dans la suite et qui est dû à M. Minkowski. Ce théorème permet de ramener à un principe fondamental et unique toute une classe de recherches de la théorie des nombres, ainsi que M. Minkowski l'a montré dans son très intéressant livre « La Géométrie des Nombres », Leipzig 1896, auquel je renvoie volontiers le lecteur.

Tout d'abord fixons quelques dénominations utiles :

On appelle *forme linéaire et homogène* à n variables une expression de la forme

$$f = a_1x_1 + a_2x_2 + \dots + a_nx_n$$

où $a_1 \dots a_n$ sont des constantes et $x_1 \dots x_n$ des variables. Lorsqu'on a un système de n formes linéaires et homogènes à n variables

$$f_i = a_{i1}x_1 + a_{i2}x_2 + \dots + a_{in}x_n$$

(pour $i = 1, 2, \dots n$) le déterminant des n^2 coefficients de ces formes

$$\Delta = (a_{11}, a_{22}, \dots a_{nn})$$

s'appelle le *déterminant des n formes*.

Le théorème de M. Minkowski s'énonce alors

Théorème I. — Si

$$f_i = a_{i1}x_1 + a_{i2}x_2 + \ldots + a_{in}x_n \ (i = 1, 2, n)$$

sont n formes linéaires et homogènes à coefficients réels et de déterminant égal à $+1$, on peut toujours trouver n valeurs rationnelles entières qui ne sont pas toutes nulles pour $x_1 \ldots x_n$ telles que la valeur absolue de chacune des formes f devienne $\leqslant 1$. C'est-à-dire telles qu'on ait à la fois

$$|f_1| \leqslant 1 \ |f_2| \leqslant 1 \ldots f_n \leqslant 1. \ (^1)$$

La démonstration que nous allons donner est due à M. Hilbert, qui a eu la bonté de la mettre à notre disposition. Il l'a donnée dans un cours fait à l'Université de Königsberg pendant l'hiver 1890-91. Je me contenterai de donner la démonstration pour le cas de $n = 3$, car dans ce livre nous n'appliquerons le théorème de Minkowski que pour $n = 2$ et $n = 3$ et que d'ailleurs le cas $n = 3$ présente déjà la démonstration dans son caractère de généralité.

Démonstration : Nous l'établirons en trois points.

1. Nous prendrons comme *forme normale* pour 3 formes $f_1 \, f_2 \, f_3$ le système

$$f_1 = \frac{x_1}{h_1} \qquad f_2 = \frac{x_2}{h_2} \qquad f_3 = c_1x_1 + c_2x_2 + h_1h_2x_3$$

où $h_1 \, h_2$ sont des entiers rationnels et $c_1 \, c_2$ des nombres réels quelconques. Nous ne restreindrons pas la généralité en supposant h_1

---

(1) Minkowski. — *Geom. d. Zahlen.*, p. 104. Dans l'ouvrage de M. Minkowski, ce théorème n'est qu'un cas particulier d'un théorème géométrique général sur un corps complètement convexe ayant un centre dans l'espace à n dimensions.

Je ne puis m'empêcher d'énoncer ce théorème en le particularisant à la géométrie plane et en anticipant sur la notion de réseau de nombres que j'exposerai dans la 3e partie de ce livre.

Dans un réseau de nombres, dont la maille fondamentale a un contenu égal à 1, supposons qu'on ait tracé une ligne convexe fermée qui ne se recoupe nulle part (par exemple, un polygone) et telle qu'un sommet du réseau soit centre de la ligne, et de façon que cette ligne renferme une surface simplement connexe. Si l'aire de ce domaine est égale à 4, il y aura à l'intérieur du contour ou sur le contour outre le centre au moins un autre sommet du réseau.

h_2 entiers positifs, sans quoi on remplacerait x_1 par $-x_1$. Nous allons d'abord démontrer que le théorème est vrai pour la forme normale.

Prenons pour x_1 un nombre du système

$$0 \pm 1 \pm 2 \dots \pm \frac{h_1}{2}$$

ou du système

$$0 \pm 1 \dots \pm \frac{h_1 - 1}{2}, \left[\frac{h_1}{2}\right] + 1$$

suivant que h_1 est pair ou impair et en même temps pour x_2 un nombre de

$$0 \pm 1 \pm 2 \dots \pm \frac{h_2}{2}$$

ou de

$$0 \pm 1 \dots \pm \frac{h_2 - 1}{2}, \left[\frac{h_2}{2} + 1\right]$$

suivant que h_2 est pair ou impair, nous aurons $(h_1 + 1)(h_2 + 1)$ systèmes de valeurs de x_1 et de x_2 pour lesquelles

$$|f_1| \leqq \frac{1}{2} \quad \text{ou} \quad \leqq \frac{1}{2} + \frac{1}{2h_1} \quad \text{et} \quad |f_2| \leqq \frac{1}{2} \text{ ou } f_2 \leqq \frac{1}{2} + \frac{1}{2h_2}.$$

A chacun de ces systèmes de valeurs de x_1, x_2 nous pouvons faire correspondre une valeur entière et rationnelle de x_3 telle que

$$f_3 = h_1 h_2 \left(\frac{c_1 x_1 + c_2 x_2}{h_1 h_2} + x_3\right)$$

ait une valeur comprise entre 0 et $h_1 h_2$, car en effet il est possible de choisir x_3 tel que

$$\frac{c_1 x_1 + c_2 x_2}{h_1 h_2} + x_3$$

soit une fraction positive comprise entre 0 et 1 et alors

$$0 < f_3 \leqq h_1 h_2.$$

Répartissons donc les $(h_1 + 1)(h_2 + 1)$ valeurs de f_3 suivant leur grandeur dans les intervalles 0 à 1, 1 à 2, 2 à 3 ... etc., de $h_1 h_2 - 1$ à $h_1 h_2$, les $(h_1 + 1)(h_2 + 2)$ valeurs seront réparties dans

dans $h_1 h_2$ intervalles, il y aura donc dans au moins un intervalle plus d'une valeur de f_3.

Supposons que pour

$$x_i = a_i \qquad x_i = a_i'$$

les valeurs

$$f_3' = c_1 a_1 + c_2 a_2 + h_1 h_2 a_3$$

et

$$f_3' = c_1 a_1' + c_2 a_2' + h_1 h_2 a_3'$$

soient dans un même intervalle, alors il est évident que

$$| f_3' - f_3'' | \leqq 1$$

ou que $f_3 \leqq 1$ pour les valeurs non nulles

$$x_i = a_i - a_i' \; (i = 1 . 2 . 3)$$

et en tenant compte de la façon dont on a déterminé a_1, a_2, a_1', a_2', on a en même temps

$$| a_1 - a_1' | h_1 \leqq | a_2 - a_2' | \leqq h_2$$

et par suite on a aussi pour

$$x_1 = a_1 - a_1' \quad \text{et} \quad x_2 = a_2 - a_2' \qquad | f_1 | \leqq 1 \; | f_2 | \leqq 1.$$

Le théorème est donc démontré pour la forme normale.

2. Soient

$$f_i = a_{i1} x_1 + a_{i2} x_2 + a_{i3} x_3 \; (i = 1 . 2 . 3)$$

trois formes linéaires à coefficients réels quelconques et de déterminant $\Delta = + 1$, nous sommes conduits à transformer cette forme en forme normale par une substitution

$$x_i = l_{i1} y_1 + l_{i2} y_2 + l_{i3} y_3 \; (i = 1 . 2 . 3) \qquad \text{(S)}$$

Si l'on remplace les x_1 on obtient des formes en y de déterminant Δ_y qui d'après un théorème connu

$$\Delta_y = (a_{11}, a_{22}, a_{33}) (l_{11}, l_{22}, l_{33}) = 1 \; (l_{11}, l_{22}, l_{33})$$

et pour que le déterminant des y soit égal à 1, il faut que la substitution (S) soit une substitution unité, c'est-à-dire

$$(l_{11}, l_{22}, l_{33}) = +1.$$

Si de plus les l_{ik} sont des entiers rationnels de déterminant

$$(l_{11}, l_{22}, l_{33}) = 1$$

les formules (S) font correspondre des valeurs entières de y à des valeurs entières de x et réciproquement. Pour que la substitution unité (S) transforme f_1 en $\frac{y_1}{h_1}$ il faut que les l_{ik} satisfassent aux équations

$$(1) \qquad (l_{11}\, l_{22}\, l_{33}) = 1$$

$$(2) \qquad a_{11}l_{11} + a_{12}l_{21} + a_{13}l_{32} = \frac{1}{h_1}$$

$$(3) \qquad a_{11}l_{12} + a_{12}l_{12} + a_{13}l_{32} = 0$$

$$(4) \qquad a_{11}l_{13} + a_{12}l_{23} + a_{13}l_{33} = 0.$$

Il serait facile de déterminer l_{ik} comme nombres entiers satisfaisant à ces équations, dans le cas où $a_{11}a_{12}a_{13}$ pourraient être supposés rationnels et premiers entre eux, ou si l'on admettait qu'ils ont un facteur rationnel commun $\frac{1}{h}$. Il n'est pas nécessaire que les a satisfaisant à ces hypothèses en général, car on peut trouver des formes qui satisfassent à ces conditions et qui diffèrent des formes données d'aussi peu que l'on veut. Cela résulte de ce qui suit.

Soit $a_{11}a_{22} - a_{21}a_{12}$ le déterminant mineur de a_{33} et qui n'est pas nul, soit δ une quantité donnée quelconque positive. On peut toujours trouver une quantité $\varepsilon < \delta$ telle qu'après une variation des coefficients $a_{11}a_{12} \ldots a_{32}$ d'une quantité $\leq \varepsilon$, il suffira de faire varier a_{33} d'une quantité au plus égale à δ pour que le déterminant Δ_ε de la nouvelle forme soit aussi égal à $+1$. En effet si chaque coefficient a_{ik} varie de $\varepsilon_{ik} < 1$, et si l'on suppose donnés tous les ε_{ik} sauf ε_{33}, la condition $\Delta_\varepsilon = 1$ donne

$$\varepsilon_{33} = \frac{\pm \varepsilon_{11}A_{11} \pm \varepsilon_{12}A_{12} + \cdots}{(a_{11} - \varepsilon_{11}, a_{22} - \varepsilon_{22} \ldots}$$

où A_{11}, A_{12} sont des nombres qui dépendent des coefficients a et

peut-être aussi des ε_{ik}. Si l'on désigne par ε la plus grande des variations ε_{ik}, on a

$$|\varepsilon_{33}| < \frac{\varepsilon A}{|(a_{11}\ a_{22})|}$$

où A est une quantité qui dépend des coefficients a et de nombres déterminés, $|\varepsilon_{33}|$ sera $< \delta$ dès que ε satisfera à la condition toujours possible $\frac{\varepsilon A}{|(a_{11}\ a_{22})|} < \delta$ et réciproquement.

Ceci posé, on fera varier les coefficients $a_{11}\ a_{12}\ a_{13}$ de la première forme f_1 le moins de ε de façon que les coefficients nouveaux soient des nombres *rationnels* de la forme

$$\frac{h_{11}}{h'} \quad \frac{h_{12}}{h'} \quad \frac{h_{13}}{h'}.$$

Puis on multipliera les numérateurs et les dénominateurs de ces fractions par une puissance assez élevée de l'entier $h_{11}h_{12}h_{13} = H$ pour que les expressions

$$\frac{H_{11}}{h_1} = \frac{h_{11}H^n \pm 1}{h'H^n} \qquad \frac{H_{12}}{h_1} = \frac{h_{12}H^n}{h'H^n} \qquad \frac{H_{13}}{h_1} = \frac{h_{13}H^n}{h'H^n}$$

diffèrent aussi de $a_{11}\ a_{12}\ a_{13}$ de moins de ε. $H_{11}\ H_{12}\ H_{13}$ n'auront certainement pas de diviseur commun, on appliquera la substitution (S) à la forme

$$\varphi_1 = \frac{H_{11}}{h_1} x_1 + \frac{H_{12}}{h_1} x_2 + \frac{H_{13}}{h_1} x_3$$

et aux formes $f_2\,f_3$, et on déterminera les l_{ik} de telle sorte que $(l_{11}\ l_{22}\ l_{23}) = 1$, et de plus

$$(1_a) \qquad H_{11}l_{11} + H_{12}l_{21} + H_{13}l_{31} = 1$$
$$(2_a) \qquad H_{11}l_{12} + H_{12}l_{22} + H_{13}l_{32} = 0$$
$$(3_a) \qquad H_{11}l_{13} + H_{12}l_{23} + H_{13}l_{33} = 0.$$

On peut toujours déterminer pour $l_{12}\ l_{22}\ l_{22} \dots l_{33}$ des valeurs rationnelles entières satisfaisant à $(2a)$ $(3a)$. On en tire alors

$$(4) \qquad \begin{aligned} H_{11} &= t\,(l_{22}l_{33} - l_{23}l_{32}) \\ H_{12} &= t\,(l_{32}l_{13} - l_{12}l_{33}) \\ H_{13} &= t\,(l_{12}l_{23} - l_{13}l_{22}) \end{aligned}$$

où t est un coefficient de proportionnalité rationnel. Mais comme H_{11}, H_{12}, H_{13} sont premiers entre eux, t ne peut être que l'inverse d'un nombre entier, on peut par avance admettre qu'on a choisi pour les l des nombres entiers premiers entre eux de façon que $t = 1$. On pourra alors satisfaire à (1_a) par les valeurs $l_{11}\, l_{21}\, l_{31}$, sans diviseur commun, car la congruence

$$H_{11}x + H_{12}y - 1 \equiv 0 \pmod{H_{13}}$$

admet des solutions.

Les valeurs des l_{ik} ainsi choisies satisfont à $(l_{11}\, l_{22}\, l_{33}) = 1$ comme il résulte des équations (1_a) et (4) lorsqu'on fait $t = 1$ dans ces dernières. Supposons que la transformation (S) nous ait donné les trois nouvelles formes

$$\text{(II)} \qquad \begin{aligned} f_1' &= \frac{y_1}{h_1} \\ f_2' &= b_{21}y_1 + b_{22}y_2 + b_{23}y_3 \\ f_3' &= b_{31}y_1 + b_{32}y_2 + b_{33}y_3. \end{aligned}$$

On déterminera tout d'abord un $\varepsilon_1 < 1$ tel qu'à des variations des coefficients $b_{21}\, b_{23}\, b_{33}$ des quantité $\leqslant \varepsilon$, correspondent pour les coefficients antérieurs a des variations $\leqslant \varepsilon$. On donnera aux $b_{21}\, b_{22}\, b_{23}$ des variations $< \varepsilon$, et on obtiendra

$$\varphi_2' = \frac{H_{21}}{h_2}y_1 + \frac{H_{22}}{h_2}y_2 + \frac{H_{23}}{h_2}y_3$$

où $H_{22}\, H_{23}$ n'ont pas de diviseur commun et où H_{21}, H_{22}, H_{23}, h_2 sont des entiers rationnels, tandis $\frac{H_{21}}{h_2}$ etc., diffèrent dès b, de moins de ε_1.

On appliquera ensuite aux formes f_1', φ_2', f_3 une substitution entière (S')

$$\text{(S')} \qquad \begin{cases} y_1 = z_1 \\ y_2 = m_{21}z_1 + m_{22}z_2 + m_{23}z_3 \\ y_3 = m_{31}z_1 + m_{32}z_2 + m_{33}z_3 \end{cases}$$

telle que $m_{22}m_{33} - m_{32}m_{33} = +1$ qui satisfait aux trois conditions suivantes.

$$(1) \qquad H_{21} + H_{22}m_{21} + H_{23}m_{31} = 0$$

$$(2) \qquad H_{22}m_{22} + H_{23}m_{32} = 0$$

$$(3) \qquad H_{22}m_{23} + H_{23}m_{33} = 0$$

On peut choisir d'une infinité de manières des m_2, m_3, entiers satisfaisant à (1b), de plus d'après la dernière équation on peut faire

$$m_{33} = + H_{12} \qquad m_{23} = - H_{23}$$

mais comme H_{12} H_{23} sont premiers entre eux on peut déterminer m_{22} m_{32} satisfaisant à (2b) et par suite à

$$m_{22}m_{33} - m_{32}m_{23} = 1.$$

La substitution (S′) nous donne alors

$$f_1'' = \frac{z_1}{h_1}$$

$$f_2'' = \frac{z_2}{h_2}$$

$$\varphi_3'' = c_{31}z_1 + c_{32}z_2 + c_{33}z_3$$

On peut dire que les formes f_1'' f_2'' résultent par la substitution (SS′) des deux formes φ_1 et φ_2 qui de leur côté proviennent des formes primitives f_1 f_2 par les variations des coefficients a_{11} a_{12} a_{13} a_{21} a_{22} a_{33} $\leqslant \varepsilon$. Si de plus on fait varier les coefficients de la 3e forme primitive f_3 de quantités $\leqslant \varepsilon$ et δ, de façon que les coefficients soient rationnels et le déterminant $\Lambda = + 1$ on obtient nne forme φ_3, laquelle par suite de la substitution (SS′) devient

$$f_3'' = c_1z_1 + c_2z_2 + h_1h_2z_3$$

car le déterminant Δ_2 de (SS′) est égal à 1. Il faut donc passer de φ_3'' à f_3'' par des variations $\leqq \varepsilon_2$.

Nous avons démontré que le théorème de Minkowski est vrai pour les formes f_1'' f_2'' f_3''. Au moyen des substitutions (S) et (S′) on obtient des valeurs de x_1 x_2 x_3 telles que le théorème s'applique aux formes φ_1 φ_2 φ_3, plus il ne nous reste qu'à démontrer que le théorème est vrai pour les formes primitives, lorsqu'il est vrai pour des formes qui en découlent par une variation aussi petite que l'on veut.

3. Faisons varier les coefficients des formes f_1 f_2 f_3 de quantités $\leqq \delta$ de façon que leur déterminant reste fini et ne devienne pas nul, et résolvons les équations $\varphi_i = w_i$ $(i = 1.2.3)$ pour des w_i, donnés situées entre — 1 et + 1, par rapport aux x, toutes les valeurs des $|x|$ seront inférieures à un nombre fini donné b différent de zéro. Mais comme il n'y a qu'un nombre *fini* de nombres

rationnels entiers $< b$, il n'y a qu'un nombre *fini* de combinaisons $x_1\ x_2\ x_3$ pour lesquelles

$$|\varphi_1| \leqq 1\ |\varphi_2| \leqq 1\ |\varphi_3| \leqq 1.$$

Admettons qu'aucun de ces systèmes ne nous donne $|f_i| \leqq 1$ on aurait pour l'un au moins des formes primitives soit f_k $|f_k| = 1 + \lambda$ avec λ positif et alors si l'on pose

$$\delta < \frac{\lambda}{3\,.\,GM}$$

où M est la valeur absolue du plus grand coefficient a_{ik} et où G a la signification indiqué plus haut on aurait toujours $\varphi_k > 1$ c'est-à-dire que le théorème ne serait pas vrai pour les formes qu'on a fait varier de quantités $\leqq \delta$. Mais on a démontré que le théorème est vrai pour ces formes il y a donc un système de valeurs de nombres entiers rationnels, tels que

$$|f_1| \leqq 1, \quad |f_2| \leqq 1, \quad |f_3| \leqq 1.$$

En général on applique le théorème de Minkowski sous la forme.

Théorème II. — Soient

$$f_i = a_{i1}x_1 + a_{i2}x_2 + a_{i3}x_3\ (i = 1, 2, 3)$$

trois formes linéaires à coefficients réels et à déterminant positif, et soient w_1, w_2, w_3 trois nombres positifs, dont le produit w_1, w_2, $w_3 = \Delta$ mais qui peuvent être qnelconques, on peut toujours trouver trois entiers rationnels x_1, x_2, x_3 pour lesquels

$$|f_1| \leqq w_1, \quad |f_2| \leqq w_2, \quad |f_3| \leqq w_3$$

le théorème se déduit immédiatement du premier, il suffit de poser

$$f_1 = w_1\varphi_1 \quad f_1 = w_2\varphi_2 \quad f_3 = w_3\varphi_3$$

alors φ_1, φ_2, φ_3, dont trois formes réelles de déterminant $\Delta = 1$. On peut donc trouver trois valeurs entières x_1, x_2, x_3 telles que

$$|\varphi_1| \leqq 1, \quad |\varphi_2| \leqq 1, \quad |\varphi_3| \leqq 1$$

et pour ces valeurs des variables on a

$$|f_1| \leqq w_1, \qquad |f_2| \leqq w_2, \qquad |f_3| \leqq w_3.$$

Finalement si l'on résout les trois équations $f_i = c_i$ de déterminant $\Delta = 1$ par rapport aux inconnus x_1, x_2, x_3 on a le

Théorème III. — Si les trois formes linéaires

$$x_i = A_{i_1}c_1 + A_{i_2}c_2 + A_{i_3}c_3 \; (i = 1 \,.\, 2 \,.\, 3)$$

ont des coefficients réels de déterminant $+ 1$, il est possible de déterminer pour c_1, c_2, c_3 des valeurs réelles comprises entre $- 1$ et $+ 1$ telles que x_1, x_2, x_3 deviennent des nombres entiers.

16. Idéaux équivalents. Classes d'idéaux des corps. *Définition*. — Deux idéaux du corps sont dits *équivalents* et on écrit

$$\mathfrak{a} \sim \mathfrak{b}$$

lorsqu'on peut trouver deux nombres du corps α et β tels que

$$(\beta)\, \mathfrak{a} = (\alpha)\, \mathfrak{b}$$

ce que nous conviendrons d'écrire

$$\frac{\mathfrak{a}}{\mathfrak{b}} = \frac{\alpha}{\beta}$$

et nous appellerons $\frac{\alpha}{\beta}$ le quotient des deux idéaux $\mathfrak{a}$ et $\mathfrak{b}$.

Lorsque $\mathfrak{a}$ est un idéal principal on écrit $\mathfrak{a} \sim (1)$.

De la définition il résulte

1. Si $\mathfrak{a} \sim \mathfrak{b}$ et $\mathfrak{b} \sim \mathfrak{c}$ $\mathfrak{a} \sim \mathfrak{c}$.

2. Si $\mathfrak{a} \sim \mathfrak{b}$ et $\mathfrak{c} \sim \mathfrak{d}$ on a aussi $\mathfrak{a}\mathfrak{c} = \mathfrak{b}\mathfrak{d}$.

3. Si $\mathfrak{a}$ et $\mathfrak{b}$ sont deux idéaux équivalent et s'il existe un idéal tel que $\mathfrak{a}\mathfrak{c}$ soit un idéal principal $\mathfrak{b}\mathfrak{c}$ est aussi un idéal principal. Kummier avait pris cette propriété comme définition de l'équivalence et c'est sous cette forme qu'on l'emploie pour reconnaître si deux idéaux sont équivalents. En effet ces deux définitions reviennent au même car si

$$\mathfrak{a}\mathfrak{c} \sim \mathfrak{b}\mathfrak{c}$$

on a

$$\mathfrak{a}\,(n\,(\mathfrak{c})) \sim \mathfrak{b}\,(n\mathfrak{c})$$

c'est-à-dire

$$\mathfrak{a} \sim \mathfrak{b}$$

4. Si $\mathfrak{a}\mathfrak{c} \sim \mathfrak{b}\mathfrak{d}$ et si $\mathfrak{a} \sim \mathfrak{b}$ aussi $\mathfrak{c} \sim \mathfrak{d}$.

5. Si $\mathfrak{a} \sim \mathfrak{b}$ on aussi $\mathfrak{a}' \sim \mathfrak{b}'$ car $n(\mathfrak{a}) \sim n(\mathfrak{b})$ c'est sur la notion d'équivalence que nous fonderons la

Définition. — Tous les idéaux équivalents à un idéal donné forment une classe d'idéaux.

D'après cela chaque idéal détermine une classe d'idéaux qui contient une infinité d'idéaux. Cependant la définition est justifiée par ce fait que tous les idéaux d'une même classe nous donnent toujours la même classe. Tous les idéaux principaux sont équivalents à l'idéal (1) et forment ensemble la *classe principale.*

Nous emploierons les majuscules latines K_1, K_2, K_3 pour désigner les classes d'un corps, en particulier la classe principale s'écrit $K = 1$. Soit $\mathfrak{a}$ un idéal de la classe K, $\mathfrak{a}_1$ un idéal de la classe K_1, $\mathfrak{b} = \mathfrak{a}\mathfrak{a}_1'$ un idéal de la classe K_2 nous écrirons symboliquement $K_2 = KK_1$. Nous pourrons donc faire des produits de classes, en remarquant qu'en particulier.

$$K = 1 \times K.$$

A chaque idéal $\mathfrak{a}$ on peut faire correspondre d'une infinité de manières un idéal $\mathfrak{a}_1$ tel $\mathfrak{a}\mathfrak{a}_1$ soit un idéal principal. A chaque classe K on peut faire correspondre une classe K_1 et une seule telle que $KK_1 = 1$. Les deux classes K et K_1 sont dites réciproques l'une de l'autre et on écrit $K_1 = K^{-1}$ $K = K_1^{-1}$.

Enfin on peut étendre l'idée de division au calcul des classes d'idéaux une classe K de k corps est dite *divisible* par une classe K_1 du même corps lorsqu'il existe dans K une classe d'idéaux K_2 tel que $K = K_1K_2$.

Nous pourrons dénombrer les classes d'idéaux grâce au théorème suivant :

Théorème fondamental. — Le nombre des classes d'un corps quadratique est toujours fini; car il y a toujours dans une classe d'idéaux au moins un idéal, dont la norme est inférieure ou au plus égal à $|\sqrt{d}|$.

Pour le démontrer nous établirons d'abord le

Lemme. Dans chaque idéal $\mathfrak{a}$ du corps K de discriminant d il y a toujours un nombre α dont la norme est en valeur absolue

$$\leqslant \left| n(\mathfrak{a}) \sqrt{d} \right|.$$

Démonstration. — Supposons qu'on ait pris pour $\mathfrak{a}$ la représentation canonique

$$\mathfrak{a} = (i, i_1 + i_2 \omega)$$

si le corps est réel nous poserons

$$(\mathrm{I}) \qquad \begin{cases} f_1 = ix \pm (i_1 + i_2 \omega) y \\ f_2 = ix \pm (i_1 + i_2 \omega') y \end{cases}$$

s'il est imaginaire

$$(\mathrm{I}') \qquad \begin{cases} f_1 = \frac{1}{\sqrt{2}} \left\{ 2ix + (2i_1 + i_2[\omega + \omega']) y \right\} \\ f_2 = \frac{1}{\sqrt{2}\sqrt{-1}} \left\{ 0 \cdot x \pm i_2 (\omega - \omega') y \right\} \end{cases}$$

et nous choisirons le signe + ou — de telle sorte que le déterminant de ces formes

$$\Delta = ii_2 \left| \sqrt{d} \right| = \left| n(\mathfrak{a}) \sqrt{d} \right|.$$

De plus dans le cas où le corps est réel, soient $\varkappa_1$, $\varkappa_2$ deux nombres réels positifs tels que

$$\varkappa_1 \varkappa_2 = \left| n(\mathfrak{a}) \sqrt{d} \right|$$

et de plus si le corps est imaginaire, soit

$$\varkappa_1 = \varkappa_2 = \varkappa.$$

D'après le théorème de Minkowski il existe des nombres rationnels entiers différents de zéro pour lesquels

$$|f_1| < \varkappa_1 \quad |f_2| < \varkappa_2$$

dans le corps réel il suffit de prendre $\alpha = f_1$, α satisfait à la condition car α est un nombre de l'idéal

$$\alpha' = f_2 \quad \text{et} \quad |n(\alpha)| \leqslant \left| n(\mathfrak{a}) \sqrt{d} \right|.$$

Dans le cas du corps imaginaire

$$\alpha = \frac{f_1 \pm \sqrt{-1}\, f_2}{\sqrt{2}}$$

est un nombre remplissant les conditions de l'énoncé, car α est un nombre de l'idéal et

$$\alpha' = \frac{f_1 \mp \sqrt{-1}\, f_2}{\sqrt{2}}$$

et de plus

$$|n(\alpha)| = \frac{1}{2}|f_1^2 + f_2^2| \leqslant \frac{1}{2}|x_1^2 + x_2^2| \leqslant x^2 \leqslant |n(\mathfrak{a})\sqrt{d}|.$$

Remarque. — Le théorème est évidemment vrai pour un idéal principal $\mathfrak{a} = (\alpha)$ il y a donc toujours dans le corps k nn nombre $\neq$ 0 et de $\pm$ 1, λ tel que $|n(\lambda)| \leqslant |\sqrt{d}|$.

Démonstration du théorème fondamental. — Soit $\mathfrak{a}$ un idéal de la classe A, et α un nombre de $\mathfrak{a}$ satisfaisant à $|n(\alpha)| \leqslant |n(\mathfrak{a})\sqrt{d}|$.

Dans la classe B réciproque de A il y a un idéal $\mathfrak{b}$ tel que $\mathfrak{a}\,.\,\mathfrak{b}\,. = (\alpha)$ mais à cause de

$$n(\mathfrak{a})\, n(\mathfrak{b}) = n(\alpha) \leqslant |n(\mathfrak{a})\sqrt{d}|$$

il en résulte

$$n(\mathfrak{b}) \leqslant |\sqrt{d}|.$$

Il y a donc dans la classe B un idéal dont la norme $\leqslant |\sqrt{d}|$ si l'on intervertit A et B on a le résultat pour A.

$\sqrt{d}$ est fini, et il n'y a qu'un nombre fini d'idéaux différents dont la norme ne dépasse pas un nombre donné, il en résulte que le nombre des classes d'idéaux est fini et qu'il est certainement $< 2|\sqrt{d}|$.

Nous emploierons constamment la lettre h pour désigner le nombre des classes d'idéaux, c'est là une constante importante du corps, nous allons rechercher sur des exemples sa détermination pratique.

Pour décider si deux idéaux sont équivalents nous appliquerons

le théorème : si $\mathfrak{a}$ et $\mathfrak{b}$ sont équivalents et si $\mathfrak{c}$ est tel que $\mathfrak{ac}$ soit un idéal principal, $\mathfrak{bc}$ est aussi un idéal principal.

Exemples pour l'équivalence :

1. Dans $k\sqrt{-5}$ on a

$$(2,\ 1+\sqrt{-5}) \sim (3,\ 1+\sqrt{5}) \not\sim (1)$$

car si on multiplie les deux membres de cette équivalence par

$$(3,\ 1-\sqrt{5})$$

il vient

$$(3,\ 1+\sqrt{-5})\,(3,\ 1-\sqrt{5}) = (3) \sim 1$$

et

$$(2,\ 1+\sqrt{-5})\,(3,\ 1-\sqrt{-5}) = (1+\sqrt{-5}) \sim 1.$$

De plus

$$(3,\ 1+\sqrt{-5}) \sim (3,\ 1-\sqrt{-5})$$

car

$$(3,\ 1+\sqrt{-5})^2 = (2-\sqrt{-5}) \sim 1.$$

2. Dans le corps

$$K(\sqrt{-23})\quad \omega = \frac{1+\sqrt{-23}}{2}$$

$$(2,\ \omega) \not\sim (2,\ \omega')$$

car

$$(2,\ \omega)^2 = (4,\ 2\omega,\ -6+\omega) = (4,\ 2-\omega) \not\sim 1$$

tandis que

$$(2,\ \omega)\,(2,\ \omega') = (2) \sim 1$$

par contre

$$(3,\ \omega) \sim (2,\ \omega')$$

car

$$(3,\ \omega)\,(2,\ \omega) = (6,\ 3\omega,\ 2\omega,\ \omega^2) = (\omega) \sim 1$$

et

$$(2,\ \omega)\,(2,\ \omega') = (2).$$

3. Dans le corps $k(\sqrt{31})$

$$(3, 1+\sqrt{31}) \not\sim (3, 1-\sqrt{31})$$

car

$$(3, 1+\sqrt{31})^2 = (9, 2-\sqrt{31}) \not\sim 1$$

par contre

$$(3, 1+\sqrt{31}) \sim (5, 1+\sqrt{31})$$

car

$$(3, 1+\sqrt{31})(5, 1-\sqrt{31}) = (4+\sqrt{31})$$

et de là il résulte évidemment

$$(3, 1-\sqrt{31}) \sim (5, 1-\sqrt{31}).$$

Exemples pour la recherche du nombre des classes.

L'algorithme d'Euclide pour la recherche des diviseurs s'applique aux corps

$$K(\sqrt{-1}) \quad K(\sqrt{-2}) \quad K(\sqrt{-3}).$$

Tous les idéaux de ces corps sont des idéaux principaux et par suite le nombre des classes dans ces corps est égal à 1.

1 a. Pour le $k(\sqrt{-5})$ on a $m = -5 \equiv 3\ (4)$, $d = -20$ et $|\sqrt{d}| < 5$ les nombres 2 et 3 peuvent être décomposés et on a

$$(2) = (2, 1+\sqrt{-5})(2, -1+\sqrt{5}) = \mathfrak{a} \cdot \mathfrak{a}'., \ \mathfrak{a} = \mathfrak{a}' \ \text{et} \ n(\mathfrak{a}) = 2$$
$$(3) = (3, 1+\sqrt{-5})(3, -1+\sqrt{-5}) = \mathfrak{b} \cdot \mathfrak{b}, \ n(\mathfrak{b}) = 3.$$

Nous avons démontré que tout idéal du corps est équivalent à l'un des idéaux (1) $\mathfrak{a}, \mathfrak{b}, \mathfrak{b}'$ car ce sont les seuls idéaux dont les normes ne dépassent pas $\sqrt{5}$. Mais comme on a montré que

$$\mathfrak{a} \sim \mathfrak{b} \sim \mathfrak{b}' \not\sim (1)$$

le nombre des classes du corps $h = 2$ et ces classes sont déterminées par les idéaux (1) et $(2, 1+\sqrt{-5})$.

2 a. Pour le corps $k(\sqrt{-23})$ $m \equiv 1\ (4)$ par suite

$$d = -23 \quad \text{et} \quad |\sqrt{d}| < 5.$$

Les nombres 2 . 3 . 4 . sont décomposables en facteurs qui ne sont pas des idéaux principaux

$$(2) = (2, \omega)(2, \omega') = \mathfrak{a} \cdot \mathfrak{a}' \quad \text{et} \quad n(\mathfrak{a}) = 2$$
$$(3) = (3, \omega)(3, \omega') = \mathfrak{b} \cdot \mathfrak{b}' \quad \text{et} \quad n(\mathfrak{b}) = 3$$

on a vu que $\mathfrak{a} \sim \mathfrak{b}'$, $\mathfrak{a}' \sim \mathfrak{b}$ et $\mathfrak{a}^2 \sim \mathfrak{a}'$
le nombre des classes est $h = 3$ et l'on peut représenter ces classes par (1), $\mathfrak{a}$, $\mathfrak{a}^2$ ou (1), $\mathfrak{b}'$, $\mathfrak{b}'^2$ ou (1), $\mathfrak{a}$, $\mathfrak{a}'$.

3*a*. Soit le corps

$$K(\sqrt{79}) \quad m \equiv 3\ (4) \quad d = 316 \quad \text{et} \quad |\sqrt{d}| < 18.$$

Parmi les nombres premiers rationnels plus petits que 18, 2 . 3 . 5 . 7 . 13 se décomposent 11 et 17 ne se décomposent pas. On trouve

$$(2) = (9 + \sqrt{79})(9 - \sqrt{79})$$
$$(3) = (3, 1 + \sqrt{79})(3, 1 - \sqrt{79})$$
$$(5) = (5, 2 + \sqrt{79})(5, 2 - \sqrt{79})$$
$$(7) = (7, 4 + \sqrt{79})(7, 4 - \sqrt{79})$$
$$(13) = (13, 1 + \sqrt{79})(13, 1 - \sqrt{79}).$$

Un calcul simple donne les égalités idéales suivantes

$$(3)(5, 2 + \sqrt{79}) = (8 - \sqrt{79})(3, 1 - \sqrt{79})$$
$$(3)(7, 4 + \sqrt{79}) = (10 - \sqrt{79})(3, 1 + \sqrt{79})$$
$$(3)(13, 1 + \sqrt{79}) = (35 - 4\sqrt{79})(3, 1 - \sqrt{79})$$

de même que celles que l'on obtient en remplaçant $\sqrt{79}$ par $-\sqrt{79}$.

En tenant compte des résultats obtenus précédemment on voit que les classes du corps $k(\sqrt{79})$ peuvent être représentées par

$$(1)\ \mathfrak{a} = (3, 1 + \sqrt{79}) \qquad \mathfrak{a}' = (3, 1 - \sqrt{79})$$

ou par

$$(1), \mathfrak{a}, \mathfrak{a}^2 \quad \text{ou} \quad 1, \mathfrak{a}', \mathfrak{a}'^2 \quad \text{et que} \quad h = 3.$$

Remarque. — La méthode que nous venons de donner suffit dans la pratique pour déterminer h, elle est suffisante même en théorie pour trouver des représentants des classes. Il existe cepen-

dant une méthode théorique complète, la méthode de « la théorie analytique des nombres » (analytische Zahlentheorie). Cette branche de l'étude des nombres a été fondée par Dirichlet [1] et construite par Dedekind, Kronecker, etc.

Les puissances consécutives d'un idéal non principal $\mathfrak{a}$

$$\mathfrak{a}, \mathfrak{a}^2, \mathfrak{a}^3, \ldots \mathfrak{a}^a$$

sont tous des idéaux différents et représentent des classes correspondantes A, A^2, A^3, ... Mais comme le nombre des classes est fini, toutes ces classes A, A^2, A^3, ... ne peuvent être indéfiniment distinctes. Désignons par A^{a+h_1} la première classe qui coïncide avec une classe précédente A^a on a $A^{a+h_1} = A^a$ et par suite $A^{h_1} = 1$ et on voit :

1. Les classes A, A^2, ... A^{h_1} sont toutes distinctes, tandis que

$$A^{1+h_1} = A^1, \quad A^{2+h_1} = A^2, \text{ etc.}$$

2. Le plus petit exposant h_1 pour lequel $A^{h_1} = 1$ est un diviseur de h, car si n et n_1 sont deux entiers inférieurs à h_1 et si l'on suppose $A^n = A^{n_1}$ il en résulte $A^{n_1 - n} = 1$ ou $h = n_1 - n > h_1$, on aurait donc déjà $A^a = A^{a+h}$ ce qui est contraire à l'hypothèse. Si les classes A, A^2, ... A^{h_1} donnent toutes les classes, on a $h_1 = h$. Supposons qu'outre ces classes il y en ait d'autres, et soit B une classe non comprise parmi les précédentes, alors

$$AB, A^2B, \ldots A^{h_1}B$$

représentent des classes distinctes entre elles et distinctes des précédentes si les classes sont épuisées on a $h = 2h$, sinon soit C une classe non comprise parmi les $2h$ précédentes et distincte de B, alors

$$AC, A^2C, \ldots A^{h_1}C$$

représentent encore h_1 nouvelles classes distinctes. La poursuite de ce raisonnement montre que $h = nh_1$.

On a comme conséquence directe de ce théorème [2].

---

(1) Voir ses œuvres complètes, t. I, p. 357 ff. et 411 ff. Voir Bachmann, *Théorie des nombres*, t. III, *Analytische Zahlentheorie*, Leipzig, 1894. Voir aussi Hilbert, *Zahlbericht*, § 79, p. 74.

(2) Ch. Hermite. — Œuvres, Paris 1905, t. I, p. 274.

Théorème. — Si p est un diviseur premier de la forme $X^2 + mY^2$, pour des nombres entiers X, Y (c'est-à-dire si p divise $X^2 + mY^2$) il y a toujours un exposant entier e, pour lequel

$$p^e = x^2 + my^2$$

peut être satisfaite par des entiers rationnels x et y.

Nous allons montrer qu'un grand nombre de théorèmes de la théorie élémentaire des nombres peuvent se généraliser dans la théorie des idéaux (¹).

Nous en indiquerons les plus connus.

17. La fonction Φ ($\mathfrak{a}$). — Dans la théorie des nombres, on désigne par φ (n) le nombre des entiers plus petits que n et premiers avec lui.

Soit $\mathfrak{a}$ un idéal quelconque du corps $k(\sqrt{m})$, nous supposerons connus les facteurs premiers de $\mathfrak{a}$, et nous chercherons le nombre des nombres du corps qui forment un système complet de restes suivant $\mathfrak{a}$ et qui sont premiers avec $\mathfrak{a}$.

Nous représenterons ce nombre par le symbole Φ ($\mathfrak{a}$) et nous poserons $\Phi(\mathfrak{a}) = 1$ pour $\mathfrak{a} = (1)$.

Tout d'abord soit un idéal premier $\mathfrak{p}$ de degré un et cherchons Φ ($\mathfrak{p}$).

On aura un système de restes complet suivont $\mathfrak{p}$ en considérant les n ($\mathfrak{p}$) nombres 0, 1, 2 ... p — 1, parmi lesquels 0 seul n'est pas premier avec $\mathfrak{p}$, on a donc

$$\Phi(\mathfrak{p}) = n(\mathfrak{p}) - 1 = n(\mathfrak{p})\left(1 - \frac{1}{n(\mathfrak{p})}\right).$$

En second lieu soit $\mathfrak{p}$ un idéal premier du second degré, un système complet de reste sera représenté par $r + s \cdot \omega$ où r et s parcourent la suite 0, 1, 2 ... p — 1 ce qui donne $n(\mathfrak{p}) = p^2$ combinaisons. Parmi ces nombres il n'y a encore qu'un 0 qui ne soit premier à $\mathfrak{p}$ et nous avons encore

$$\Phi(\mathfrak{p}) = n(\mathfrak{p}) - 1 = n(\mathfrak{p})\left(1 - \frac{1}{n(\mathfrak{p})}\right).$$

Si d'autre part $\mathfrak{p}$ est un idéal premier du second degré et soit

(¹) Dirichlet-Dedekind. — Vorles. Supplement. XI, p. 564 et 567-573.

$\mathfrak{a} = \mathfrak{p}^k$, $r + s\omega$ forme encore un système complet de restes suivant $\mathfrak{p}^k$ en mettant pour r et s les nombres 1, 2 ... p, ... p^k ce qui donne p^{2k} combinaisons. Mais parmi ces nombres ceux (et ceux-là seulement) qui sont obtenus en remplaçant dans $a + b\omega$, a et b à la fois par deux nombres de la suite $1p, 2p \ldots p^{k-1} \cdot p$. dans toutes leurs combinaisons possibles ne sont pas premiers avec $\mathfrak{p}$. Il y en a $p^{k-1} \cdot p^{k-1} = p^{2k-2}$, on a donc pour $\Phi(\mathfrak{a})$

$$\Phi(\mathfrak{p}^k) = n(\mathfrak{p}^k) - n(\mathfrak{p}^{k-1}) = n(\mathfrak{p}^k)\left(1 - \frac{1}{n(\mathfrak{p})}\right).$$

L'examen d'un idéal premier de degré un, donne le même résultat, par un raisonnement analogue.

Pour arriver au cas général nous supposerons $\Phi(\mathfrak{a})$ connu dans le cas $\mathfrak{a} = \mathfrak{p}_1^{k_1} \ldots \mathfrak{p}_n^{k_n}$ c'est-à-dire dans le cas où $\mathfrak{a}$ contient n facteurs premiers différents et nous allons chercher à déterminer $\Phi(\mathfrak{a}_1)$ dour $\mathfrak{a}_1 = \mathfrak{a}\mathfrak{p}^k$ en supposant $\mathfrak{p}$ premier avec $\mathfrak{a}$.

Supposons $\mathfrak{a}$ mis sous la forme normale

$$\mathfrak{a} = (a, a_1 + a_2\omega)$$

et

$$\mathfrak{p}^k = (i, i_1 + i_2\omega)$$

a et i sont certainement premiers entre eux, car $\mathfrak{a}$ et $\mathfrak{p}$ le sont

$$\mathfrak{a}_1 = \mathfrak{a}\mathfrak{p}^k = (ai, \bar{a} + a_2 i_2\omega)$$

si l'on remarque que

$$n(\mathfrak{a}_1) = n(\mathfrak{a})\, n(\mathfrak{p}^k) = ai,\ a_2 i_2.$$

On obtient un système de restes complet suivant $\mathfrak{a}$, en remplaçant dans $r + s\omega$, r par 1, 2, ... a et s par 1, 2 ... a_2 et de même on obtient un système de restes complet suivant $\mathfrak{a}_1$ en remplaçant dans $\bar{r} + s\omega$, $\bar{r}$ par 1, 2 ... ai et s par 1, 2 ... $a_2 i_2$.

Dans l'ensemble de ces nombres il y en a $ii_2\,\Phi(\mathfrak{a})$ qui sont premiers avec $\mathfrak{a}_1$ on les reconnaît en écrivant les nombres r, s, par ordre de grandeur croissante et en les répartissant en i, i_2 intervalles de a et de a_2 nombres consécutifs.

Parmi ces $i\,i_2\,\Phi(\mathfrak{a}) = n(\mathfrak{p}^k)\,\Phi(\mathfrak{a})$ nombres il y a encore des nombres contenant le facteur $\mathfrak{p}$ une ou plusieurs fois et d'ailleurs pre-

miers avec $\mathfrak{a}$. Il est facile de les compter, il suffit de voir quels sont les nombres divisibles par $\mathfrak{p}$. Il y en a un nombre égal à celui d'un système de rester complet suivant

$$\frac{\mathfrak{a}_1}{\mathfrak{p}} = a\mathfrak{p}^{k-1}$$

et premier avec a c'est-à-dire comme nous venons de le voir $n(\mathfrak{p}^{k-1})\,\Phi\,\mathfrak{a}$.

C'est-à-dire que

$$\Phi(\mathfrak{a}_1) = n(\mathfrak{p}^k)\,\Phi(\mathfrak{a}) - n(\mathfrak{p}^{k-1})\,\Phi(a)$$
$$\Phi(\mathfrak{a}_1) = \Phi(\mathfrak{a})\,n(\mathfrak{p}^k)\left(1 - \frac{1}{n(\mathfrak{p})}\right).$$

C'est là une formule de récurrence qui donne Φ pour un idéal contenant $n + 1$ facteurs premiers lorsqu'on courait Φ' pour un idéal qui en contient n. D'ailleurs on connait $\Phi(\mathfrak{p}^k)$ on aura donc si $\mathfrak{a} = \mathfrak{p}_1^{k_1} \ldots \mathfrak{p}_n^{k_n}$

$$\Phi(\mathfrak{a}) = n(\mathfrak{a})\left(1 - \frac{1}{n(\mathfrak{p}_1)}\right)\left(1 - \frac{1}{n(\mathfrak{p}_1)}\right)\cdots\left(1 - \frac{1}{n(\mathfrak{p}_n)}\right)$$

de là résulte d'ailleurs le

Théorème. — Soit $\mathfrak{a} = \mathfrak{a}_1\mathfrak{a}_2$ ou $\mathfrak{a}_1$ et $\mathfrak{a}_2$ sont des idéaux premiers entre eux on a

$$\Phi(\mathfrak{a}) = \Phi(\mathfrak{a}_1) \times \Phi(\mathfrak{a}_2).$$

Théorème. — Si l'on donne à $\mathfrak{t}$ successivement toutes les valeurs des idéaux qui divisent $\mathfrak{a}$, on a

$$\sum \Phi(\mathfrak{t}) = n(\mathfrak{a})$$

Démonstration : Supposons tout d'abord $\mathfrak{a} = \mathfrak{p}^k$, alors

$$1, \mathfrak{p}, \mathfrak{p}^2 \ldots \mathfrak{p}^k$$

sont tous des idéaux diviseurs de $\mathfrak{a}_1$ et on a

$$\sum \Phi(\mathfrak{t}) = 1 + \Phi(\mathfrak{p}) + \Phi(\mathfrak{p}^2) + \ldots + \Phi(\mathfrak{p}^k)$$
$$\sum \Phi(\mathfrak{t}) = 1 + \left(1 - \frac{1}{n(\mathfrak{p})}\right)[n(\mathfrak{p}) + n(\mathfrak{p}^2) + \ldots n(\mathfrak{p}^k)]$$
$$= 1 + \frac{n(\mathfrak{p}) - 1}{n(\mathfrak{p})} \times \frac{(n(\mathfrak{p}))^{k+1} - n(y)}{n(\mathfrak{p}) - 1} = (n(\mathfrak{p}))^k = n(\mathfrak{p}^k)$$

Si maintenant l'on a d'une façon générale $\mathfrak{a} = \mathfrak{p}_1^{k_1} \dots \mathfrak{p}_n^{k_n}$ on voit que tous les diviseurs de a sont les termes des produits symboliques :

$$(1 + \mathfrak{p}_1 + \dots \mathfrak{p}_1^{k_1})(1 + \mathfrak{p}_2 + \dots \mathfrak{p}_2^{k_2}) \dots (1 + \mathfrak{p}_n + \dots + \mathfrak{p}_n^{k_n}).$$

D'après ce qui précède $\sum \Phi(\mathfrak{t})$ est égal à

$$1 + \sum_1^n \Phi(\mathfrak{p}_i) + \sum_1^n \Phi(\mathfrak{p}_i^2) + \dots + \sum_1^n \Phi(\mathfrak{p}_i \mathfrak{p}_k) + \dots \sum_1^n \Phi(\mathfrak{p}_i^{k_i})$$

qui est égale au produit

$$\begin{aligned} \sum (\Phi(\mathfrak{t}) = & (1 + \Phi(\mathfrak{p}_1) + \dots + \Phi(\mathfrak{p}_1^{k_1})) \\ & .\,(1 + \Phi(\mathfrak{p}_2) + \dots + \Phi(\mathfrak{p}_2^{k_2})) \\ & .\quad .\quad .\quad .\quad .\quad .\quad .\quad .\quad .\quad . \\ & .\,(1 + \Phi(\mathfrak{p}_n) + \dots + \Phi(\mathfrak{p}_n^{k_n})) \\ = & \, n(\mathfrak{p}_1^{k_1}) \dots n(\mathfrak{p}_n^{k_n}) = n(\mathfrak{a}). \end{aligned}$$

On a donc pour les idéaux un théorème analogue au théorème sur les nombres rationnels.

18. Le théorème de Fermat pour les idéaux. — *Théorème.* Soit $\mathfrak{a}$ un idéal du corps $k(\sqrt{m})$ et α un nombre entier du corps premier avec $\mathfrak{a}$ on a

$$\alpha^{\Phi(\mathfrak{a})} \equiv 1 \; (\mathfrak{a}).$$

Démonstration. — Soient $\rho_1, \rho_2 \dots \rho_\nu$ les $\nu = \Phi(\mathfrak{a})$ nombres qui forment un système de restes complet suivant $\mathfrak{a}$ et qui sont premiers avec $\mathfrak{a}$, et soient

$$(C) \qquad \left\{ \begin{array}{l} \rho_1 \alpha \equiv \sigma_1, \; (\mathfrak{a}) \\ \rho_2 \alpha \equiv \sigma_2, \; (\mathfrak{a}) \\ .\quad .\quad .\quad .\quad .\quad . \\ \rho_\nu (a) \equiv \sigma_\nu, \; (\mathfrak{a}) \end{array} \right.$$

les $\sigma_1, \sigma_2 \dots \sigma_\nu$ appartiennent à leur tour au même système de restes complet que les ρ. Deux quelconques de ces σ ne peuvent être congrues suivant $\mathfrak{a}$ sans quoi on aurait, si

$$\sigma_\lambda \equiv \sigma_\mu, \; (\mathfrak{a})$$

aussi

$$\alpha(\rho_\lambda - \rho_\mu) \equiv 0, \ (\mathfrak{a})$$

puisque α est premier avec $\mathfrak{a}$. De plus aucun σ_λ ne peut avoir avec $\mathfrak{a}$ un facteur premier $\mathfrak{t}$ sans quoi comme

$$(\rho_\lambda \alpha - \sigma_\lambda) = \mathfrak{t} \cdot \mathfrak{b}$$

on en déduirait que $\mathfrak{t}$ divise $\rho_\lambda \alpha$ et par suite ρ_λ ce qui est contraire à l'hypothèse

Les nombres $\sigma_1, \sigma_2 \ldots \sigma_\nu$ sont donc dans un ordre quelconque les nombres

$$\rho_1, \rho_2 \cdots \rho_\nu$$

et l'on a

$$\rho_1, \rho_2 \ldots \rho_\nu \alpha^{\Phi(\mathfrak{a})} \equiv \sigma_1, \sigma_2 \ldots \sigma_\nu \ (\mathfrak{a})$$

c'est-à-dire

$$\alpha^{\Phi(\mathfrak{a})} \equiv 1 \ (\mathfrak{a})$$

Conséquence. I. — Soit $\mathfrak{p}$ un idéal premier de degré f ($f = 1$ ou $= 2$ du corps $k(\sqrt{m})$ et α un entier du corps non divisible par $\mathfrak{p}$, on a toujours

$$\alpha^{p^f - 1} \equiv 1 \ (\mathfrak{p})$$

et on a quel que soit α

$$\alpha^{p^f} \equiv \alpha \ (\mathfrak{p})$$

II. Soit α un nombre entier du corps qui n'est pas divisible par l'idéal premier $\mathfrak{p}$ et soit e le plus petit exposant entier rationnel tel que

$$\alpha^e \equiv 1 \ (\mathfrak{p}$$

e est un diviseur de $p^f - 1$.

Démonstration. Admettons que e ne divise pas $p^f - 1$, et soit e_1 le plus grand commun diviseur de e et de $p^f - 1$, alors $e_1 < e$ et l'on peut trouver deux entiers rationnels tels que

$$ex + (p^f - 1) y = e_1$$

et en résultera que

$$\alpha^{ex} \equiv 1 \ \ \mathfrak{p})$$
$$\alpha^{(p^f - 1)y} \equiv 1 \ (\mathfrak{p})$$

et par suite

$$\alpha^{e_1(p^f-1)} \equiv 1\ (\mathfrak{p})$$

c'est-à-dire

$$\alpha^{e_1} \equiv 1\ (\mathfrak{p})$$

$e_1 < e$ — ce qui est contraire à l'hypothèse. Il faut donc que e_1 divise $p^f - 1$.

III. On a toujours

$$\alpha^{p^f-1} \equiv 1\ (\mathfrak{p})$$

Définition

$$\alpha\xi^g + \alpha_1\xi^{g-1} \ldots + \alpha_g \equiv 0\ (\mathfrak{a})$$

sera dite une congruence de degré g si α n'est pas divisible par $\mathfrak{a}$; ρ est une racine de cette congruence, si ρ mis à la place ξ rend le premier membre congru à $\mathfrak{a}$.

Théorème. — Une congruence de degré g suivant le module $\mathfrak{p}$

$$f(\xi) = \alpha\xi^g + \ldots + \alpha_g \equiv 0\ (\mathfrak{p})$$

peut avoir au plus g racines incongrues suivant $\mathfrak{p}$.

Démonstration : Soit ρ_1 une racine de la congruence on a

$$f(\rho_1) \equiv 0\ (\mathfrak{p})$$

et

$$f(\xi) \equiv f(\xi) - f(\rho_1) = (\xi - \rho_1) f_1(\xi) \equiv 0\ (\mathfrak{p})$$

où $f_1(\xi)$ est de degré $g - 1$. Soient alors $\rho_1\ \rho_2 \ldots \rho_g$, g racines incongrues suivant $\mathfrak{p}$, on a

$$f(\xi) = \alpha(\xi - \rho_1)(\xi - \rho_2) \ldots (\xi - \rho_g) \equiv 0\ (\mathfrak{p})$$

un nombre ξ ne peut satisfaire à cette congruence que si $\mathfrak{p}$ divise l'un des g facteurs, c'est-à-dire si $\xi - \rho_x \equiv 0\ (\mathfrak{p})$.

Ce qui démontre le théorème.

19. Des racines primitives suivant un idéal premier. — Soit α un entier qui n'est pas divisible par l'idéal premier $\mathfrak{p}$ que nous supposons de degré f. Soit par exemple α un nombre du système complet de restes le plus simple suivant $\mathfrak{p}$. Nous venons de

voir qu'il existera toujours un diviseur rationnel e de $p^f - 1$, tel que

$$\alpha^e \equiv 1 \ (\mathfrak{p}).$$

Soit e le plus petit nombre tel que cette congruence soit vérifiée les nombres $\alpha \ \alpha^2 \ldots \alpha^{e-1}$ seront tous incongrus suivant le module $\mathfrak{p}$, car si on avait

$$\alpha^{e_1} \equiv \alpha^{e_2} \ (\mathfrak{p}) \qquad e_1 \text{ et } e_1 \leqq e - 1$$

on aurait

$$\alpha^{e_2}\left(\alpha^{e_1 - e_2} - 1\right) \equiv 0 \ (\mathfrak{p}) \qquad \alpha^{e_1 - e_2} \equiv 1 \ (\mathfrak{p})$$

et comme $e_1 - e_2 < e$, ceci serait contraire à l'hypothèse.

Nous dirons que α appartient à l'exposant e.

Un nombre π du corps qui appartient à l'exposant $p^f - 1$ sera dit un nombre primitif suivant l'idéal premier $\mathfrak{p}$. Les nombres

$$\pi, \pi^2, \pi^3 \ldots \pi^{p^f - 1}$$

représenteront alors des nombres incongrus suivant $\mathfrak{p}$, et premiers avec $\mathfrak{p}$, ou encore tous les nombres d'un système complet de restes qui sont premiers avec $\mathfrak{p}$.

Il faut démontrer l'existence de ces nombres primitifs $\mathfrak{p}$ étant donné. Cette démonstration est possible, on peut même, en suivant un procédé de Gauss, démontrer le théorème ainsi généralisé.

Théorème. — Soit e un facteur premier rationnel de $p^f - 1$ et $\mathfrak{p}$ un idéal premier de degré f qui divise p, un système complet de restes suivant $\mathfrak{p}$ contient toujours $\varphi(e)$ nombres appartenant à l'exposant e.

Démonstration : Nous démontrerons d'abord que s'il existe un nombre appartenant à l'exposant e, il en existe toujours $\varphi(e)$ et $\varphi(e)$ seulement, incongrus suivant le module $\mathfrak{p}$.

En effet soit r un nombre de la suite $1, 2 \ldots (e - 1)$ premier avec e, le nombre α^r appartient à l'exposant e et ne peut appartenir à un exposant moins élevé. D'après l'hypothèse

$$(\alpha^e)^r \equiv 1 \ (\mathfrak{p}) \qquad \text{c'est-à-dire} \qquad (\alpha^r)^e \equiv 1 \ (\mathfrak{p}).$$

De plus comme r est premier avec e, on ne peut avoir

$$(\alpha^r)^{e_1} \equiv 1 \ (\mathfrak{p})$$

que si $re_1 \equiv 0\ (e)$, on a plutôt $e_1 \equiv 0\ (e)$, c'est-à-dire si e_1 est un multiple de e il faut donc que e_1 soit au moins égal à e. Si donc on remplace n par tous les nombres de la suite 1, 2 ... e — 1 qui sont premiers avec e, on obtient $\varphi(e)$ nombres différents suivant le module $(\mathfrak{p})$ et qui appartiennent à l'exposant e.

Il n'y a pas d'autres nombres que ceux-là qui appartiennent à l'exposant e, un pareil nombre devrait satisfaire à la congruence

$$\xi^e \equiv 1\ (\mathfrak{p}).$$

Cette congruence admet les e racines

$$\alpha,\ \alpha^2\ \dots\ \alpha^e$$

incongrues suivant $(\mathfrak{p})$, et ne peut en admettre d'autres puisqu'elle est de degré e.

Les puissances α^s dont l'exposant s a avec e un diviseur commun e appartiennent à l'exposant

$$e_1 = \frac{e}{e}\quad e_1 < e.$$

Nous achèverons la démonstration ainsi qu'il suit.

Chacun des p^f — 1 nombres incongrus d'un système complet de restes suivant $\mathfrak{p}$ appartient à un certain diviseur de p^f — 1. Soient $t_1, t_2 \dots t_m$ tous les diviseurs de p^f — 1, on a

$$\varphi(t_1) + \varphi(t_2) + \dots + \varphi(t_m) = n(\mathfrak{p}) - 1 = p^f - 1.$$

Mais

$$\sum \varphi(t) = n(\mathfrak{p}) - 1$$

que si t représente successivement tous les diviseurs de $n(\mathfrak{p})$ — 1. Il ne peut donc y avoir de diviseur auquel n'appartient aucun nombre, et en particulier il y a exactement

$$\varphi(n - 1) = \varphi(p^f - 1)$$

nombres primitifs incongrus suivant $\mathfrak{p}$.

De ce théorème nous tirerons une généralisation du théorème de Wilson.

Théorème. — Soit $\rho_1, \rho_2 \dots \rho_k$ les nombres incongrus d'un sys-

tème de restes complets suivant un idéal premier $\mathfrak{p}$ qui ne divise pas 2, on a

$$\rho_1, \rho_2 \dots \rho_\nu \equiv -1 \ (\mathfrak{p}).$$

Démonstration : π une racine primitive suivant $\mathfrak{p}$, on peut poser

$$\rho_1 \equiv \pi^{e_1} \ (\mathfrak{p})$$

$$\cdot \quad \cdot \quad \cdot \quad \cdot$$

$$\cdot \quad \cdot \quad \cdot \quad \cdot$$

$$\rho_\nu \equiv \pi^{e_\nu} \ (\mathfrak{p})$$

ou $e_1, e_2 \dots e_\nu$ sont les nombres de la suite $1, 2 \dots n(\mathfrak{p}) - 1$, pris dans un certain ordre. On a

$$\rho_1 \rho_2 \cdots \rho_\nu \equiv \pi^{\frac{n(\mathfrak{p}) - 1}{2} n(\mathfrak{p})} \ (\mathfrak{p})$$

mais comme π est racine primitive, on a

$$\pi^{\frac{n(\mathfrak{p}) - 1}{2}} \equiv -1 \ (\mathfrak{p})$$

et de plus comme $n(\mathfrak{p})$ est impair, on a

$$\rho_1, \rho_2 \cdots \rho_\nu \equiv -1 \ (\mathfrak{p}).$$

Le théorème de Wilson, nous donne la condition de possibilité pour la congruence

$$\xi^2 \equiv -1 \ (\mathfrak{p})$$

où $\mathfrak{p}$ est premier avec (2), ou plutôt elle nous permet de trouver les modules $\mathfrak{p}$ pour lesquels cette congruence est possible.

La congruence

$$\xi^2 \equiv -1$$

admet toujours une solution dans le corps $k(\sqrt{-1})$ il ne sera pas question de ce corps dans ce qui suit.

Soit d'abord $\mathfrak{p}$ un idéal du premier degré les nombres

$$1, 2 \dots p - 1$$

ou encore

$$-\frac{p-1}{2}, -\frac{p-2}{2} \dots -2, -1, 1, 2 \dots \frac{p-3}{3}, \frac{p-1}{2},$$

forment un système complet de restes.

On a alors

$$\rho_1 . \rho_2 \dots \rho = (-1)^{\frac{p-1}{2}} \left(1 . 2 . 3 \dots \frac{p-1}{2}\right)^2 = (p-1)^{\frac{p-1}{2}} \mu^2,$$

et par suite

$$(-1)^{\frac{p-1}{2}} \mu^2 \equiv -1 \; (\mathfrak{p})$$

Le nombre μ est donc une solution de la congruence dans le cas où $p \equiv 1 \; (4)$ et dans ce cas seulement.

Supposons maintenant que $\mathfrak{p}$ est un idéal du 2ᵉ degré les nombres $r + s\omega$, pour

$$r, s = -\frac{p-1}{2}, -\frac{p-3}{2} \dots -2, -1, 1, 2 \dots \frac{p-1}{2},$$

avec les nombres

$$-\frac{p-1}{2}, -\frac{p-3}{2} \dots -1, 1, \dots \frac{p-1}{2},$$

$$-\frac{p-1}{2}\omega \dots \frac{p-1}{2}\omega$$

représentent un système complet de restes et l'on a

$$\rho_1 \rho_2 \dots \rho_\nu = (-1)^{\frac{(p-1)^2}{2} + p - 1} \left(1 . 2 . 3 \dots \frac{p-1}{2}\right)^4 \omega^{p-1} \prod\prod (r_1 - s_1\omega)^2$$

ou $\prod\prod$ est le produit de toutes les combinaisons pour $r_1 \dots$ de 1 à $\frac{p-1}{2}$ et pour s_1, de

$$-\frac{p-1}{2} \text{ à } -\frac{p-1}{2}.$$

Comme p est impair $p - 1$ est pair

$$\frac{(p-1)^2}{2} + p - 1 = (p-1)\left(1 + \frac{p-1}{2}\right)$$

est pair, donc le second membre est le carré d'un nombre du corps

$$\rho_1, \rho_2 \dots \rho_\nu = \mu^2$$

et par suite

$$\alpha^2 \equiv -1 \ (\mathfrak{p}).$$

La congruence

$$\xi^2 \equiv -1 \ (\mathfrak{p})$$

est toujours possible pour un module premier $\mathfrak{p}$ du second degré.

20. Les congruences linéaires suivant des idéaux. — Nous appellerons congruence linéaire ou congruence du premier degré une congruence de la forme

$$\alpha\xi \equiv \beta \ (\mathfrak{j}).$$

Sous quelles conditions une pareille congruence admet-elle des solutions :

1re *Hypothèse*. — L'idéal (α) et l'idéal $\mathfrak{j}$ sont premiers entre eux. Si l'on remplace ξ successivement par tous les nombres d'un système complet de restes ρ suivant $\mathfrak{j}$ on obtient les nombres

$$\alpha\rho_1, \ \alpha\rho_2 \ \ldots \ \alpha\rho_\nu$$

qui forment à leur tour un système complet de restes suivant $\mathfrak{j}$. Le nombre β est congru suivant $\mathfrak{j}$ à un de ces nombres et à un seul.

Si

$$\alpha\rho \equiv \beta \ (\mathfrak{j})$$

ρ est une solution de la congruence et la seule solution située dans le système complet de restes considéré. Tout nombre de la forme

$$\rho + gi + f(i_1 + i_2\omega)$$

est une solution de la congruence si i et $i_1 + i_2\omega$ sont les nombres de la base normale de l'idéal $\mathfrak{j}$.

Le théorème de Fermat nous donne ρ sous une forme plus précise

$$\alpha^{\Phi(\mathfrak{j})} \equiv 1 \ (\mathfrak{j})$$

$$\xi \equiv \alpha^{\Phi(\mathfrak{j})-1} \beta \ (\mathfrak{j})$$

on a donc

$$\rho \equiv \beta\alpha^{\Phi(\mathfrak{j})-1}$$

Ces résultats sont encore vrais si α et $\mathfrak{j}$ étant premiers entre eux β désigne une unité du corps (Voir plus loin n° 22).

Ces considérations sont analogues à celles que nous avons faites pour résoudre en nombre rationnel l'équation indéterminée

$$ax + by = 1.$$

Mais tandis que celle-ci peut être résolue par des développements en fractions continues il n'est plus de même pour des nombres du corps quadratique car l'algorithme d'Euclide ne vaut plus.

2me *Hypothèse.* — Considérons maintenant le cas général où (α et $\mathfrak{j}$ admettent un *p.g.c.d.* diviseur idéal $\mathfrak{d}$. La congruence

$$\alpha\xi \equiv \beta \ (\mathfrak{j})$$

n'est possible que si $\mathfrak{d}$ divise β car si l'on a

$$(\alpha\xi - \beta) = \mathfrak{t}\mathfrak{j} = \mathfrak{t}\mathfrak{j}\mathfrak{d}$$
$$\alpha\xi - \beta \equiv - \beta \equiv 0 \ (\mathfrak{d})$$

Et si la condition $\beta \equiv 0 \ (\mathfrak{d})$ est satisfaite la congruence admet des solutions. En effet soit $\mathfrak{j} = \mathfrak{j}^* \mathfrak{d}$ de plus $(\alpha) = \mathfrak{a}\mathfrak{d}$ et $\beta = \mathfrak{b}\mathfrak{d}$, par hypothèse α et $\mathfrak{j}^*$ sont premiers entre eux. On peut toujours trouver un entier δ du corps tel que (δ) soit divisé par $\mathfrak{d}$ et non par une puissance supérieure et tel

$$\frac{(\delta)}{\mathfrak{d}} = \mathfrak{d}_1$$

soit premier avec $\mathfrak{j}$ (et c'est un théorème que l'on démontre rigoureusement dans la théorie analytique des nombres).

De plus choisissons dans l'idéal $\mathfrak{d}_1$ un nombre λ premier avec $\mathfrak{j}$ ce qui doit être possible d'après la façon dont on a déterminé $\mathfrak{d}$, et posons

$$\alpha_1 = \frac{\alpha\lambda}{\delta}\quad \beta_1 = \frac{\beta\lambda}{\delta}.$$

Les nombres α_1, β_1 sont des nombres entiers du corps et si la congruence

$$\alpha\xi \equiv \beta \ (\mathfrak{j})$$

admet une solution entière $\xi = \rho$ dans le corps k ce nombre satisfait aussi à

$$\alpha_1\xi \equiv \beta_1 \ (\mathfrak{j}^*)$$

et réciproquemment car si

$$\alpha\rho \equiv \beta\ (\mathfrak{j})$$
$$\lambda\alpha\rho \equiv \lambda\beta\ (\mathfrak{j})$$

ou

$$\delta\alpha_1\rho \equiv \delta\beta_1\ (\mathfrak{j})$$
$$\alpha_1\rho \equiv \beta_1\ (\mathfrak{j}^*)$$

réciproquemment car si

$$\alpha_1\rho \equiv \beta_1\ (\mathfrak{j}^*) \qquad \delta\alpha_1\rho \equiv \delta\beta\ (\mathfrak{j}_1)$$

ou

$$\lambda\alpha_1\rho \equiv \delta\beta_1\ (\mathfrak{j})$$
$$\alpha_1\rho \equiv \beta_1\ (\mathfrak{j})$$

réciproquemment si $\alpha_1\rho \equiv \beta\ (\mathfrak{j}^*)$ $\delta\alpha\rho_1 \equiv \delta\beta_1\ (\mathfrak{j})$ ou

$$\lambda\alpha\rho \equiv \lambda\beta\ (\mathfrak{j})$$

et comme λ est premier avec $\mathfrak{j}$

$$\alpha\rho \equiv \beta\ (\mathfrak{j}).$$

Mais comme α_1 et $\mathfrak{j}^*$ sont premiers entre eux

$$\alpha_1\xi - \beta_1 \equiv 0\ (\mathfrak{j}^*)$$

admet une solution entière $\xi = \rho$ et la congruence

$$\alpha\xi - \beta \equiv 0\ (\mathfrak{j})$$

admet aussi la solution ρ. On peut toujours prendre pour ρ un nombre du système complet de reste le plus simple suivant $\mathfrak{j}^*$ et alors toutes les relations de la congruence primitive sont comprises dans la formule

$$\xi = \rho + gi^* + f\,(i_1^* + i_2^*\omega)$$

ou i^* $i_1^* + i_2^*\,\omega$ sont les nombres de base de $\mathfrak{j}^*$ et g, f des nombres entiers rationnels positifs ou négatifs. Si l'on pose de même

$$\mathfrak{j} = (i_1 i_1 + i_2\,\omega)$$

il y a parmi les nombres ξ évidemment

$$\frac{ii_2}{i^* i_2^*} \text{ ou } n\ (\mathfrak{d})$$

nombres incongrues suivant le module $\mathfrak{j}$ et l'on peut formuler le théorème ainsi qu'il suit :

Théorème. — Une congruence linéaire

$$\alpha\xi \equiv \beta\ (\mathfrak{j})$$

n'admet pour solution un nombre entier du corps que lorsque le plus grand commun diviseur $\mathfrak{d}$ de (α) et de $\mathfrak{j}$ divise (β) et alors la congruence admet $n\ (\mathfrak{d})$ solutions.

Ce théorème correspond au théorème relatif à une équation indéterminée en nombres rationnels. On peut d'ailleurs dire l'équation indéterminée

$$\alpha\xi + \gamma\eta = \beta$$

où α, β, γ sont des entiers du corps $k(\sqrt{m})$ n'admet des solutions (et alors en nombre infini) que si le plus grand commun diviseur idéal de (α) et de (γ) divise aussi (β).

Il est bon aussi de démontrer un théorème relatif à des congruences simultanées, dont voici le cas le plus simple.

Théorème. — Soit $\mathfrak{a}$ et $\mathfrak{a}_1$ deux idéaux premiers entre eux et soient α_1, α_2, deux nombres quelconques du corps. il y a toujours un nombre entier ξ du corps satisfaisant simultanément à

$$\xi \equiv \alpha_1\ (\mathfrak{a}_1) \qquad \xi \equiv \alpha_2\ (\mathfrak{a}_2).$$

Démonstration. — Soit ρ une solution de $\xi \equiv \alpha_1\ (\mathfrak{a}_1)$ et soit

$$\mathfrak{a}_1 = (a,\ a_1 + a_2\omega).$$

On aura toutes les solutions de cette congruence par la formule

$$\xi = \rho + \sigma a + \tau\,(a_1 + a_2\omega)$$

où σ et τ sont des entiers du corps. Pour que ξ satisfasse à la seconde congruence il faut choisir σ et τ de telle sorte que

$$\rho + \sigma a + \tau\,(a_1 + a_2\omega) \equiv \alpha_2,\ (\mathfrak{a}_2)$$
$$\sigma a + \tau\,(a_1 + a_2\omega) \equiv \alpha_2 - \rho,\ (\mathfrak{a}_2)$$

posons

$$\sigma = A\xi_1, \qquad \tau \equiv B\xi_1.$$

et choisissons les nombres entiers rationnels A, B, tels que

$$Aa + B\,(a_1 + a_2\omega) = \alpha_1,$$

soit premier avec $\mathfrak{a}_2$) ce qui est toujours possible car α_1^* est un nombre de $\mathfrak{a}_1$, et $\mathfrak{a}_1$, $\mathfrak{a}_2$ sont premiers entre eux.

Il nous faudra déterminer ξ_1, tel que

$$\alpha_1^* \xi_1 \equiv \alpha_2 - \rho, (\mathfrak{a}_2)$$

et alors σ, τ donneront la valeur cherchée de ξ.

On ramène facilement à la forme précédente les congruences

$$\varkappa_1 \xi \equiv \alpha_1, (\mathfrak{a}_1) \quad \varkappa_2 \xi \equiv \alpha_2, (\mathfrak{a}_2)$$

qui en apparence sont plus générales.

Si $\varkappa_1$ est premier avec $\mathfrak{a}_1$, $\varkappa_2$ premier avec a_2, il suffit de multiplier les deux membres de la première congruence par $\varkappa_1^{\Phi(\mathfrak{a}_1)-1}$, ceux de la seconde par $\varkappa_2^{\Phi(\mathfrak{a}_2)-1}$ pour ramener au cas précédent. On trouvera facilement les conditions nécessaires et suffisantes pour la résolution lorsque $\varkappa_1$ n'est pas premier avec $\mathfrak{a}_1$ et lorsque $\varkappa_2$ n'est pas premier avec $\mathfrak{a}_2$.

21. Les congruences quadratiques et le symbole $\left(\frac{\alpha}{\mathfrak{p}}\right)$. — La congruence la plus générale suivant le module $\mathfrak{p}$, est de la forme

(1) $$\alpha\xi^2 + 2\alpha_1\xi + \alpha_2 \equiv 0 \ (\mathfrak{p}),$$

où α_1, α_2, α_3 sont des nombres quelconques du corps. Si α_1, α_2, α_3 sont premiers avec $\mathfrak{p}$, cette congruence admet une racine dès que la congruence

$$\alpha\,(\alpha\xi^2 + 2\alpha_1\xi + \alpha_2) \equiv 0 \ (\mathfrak{p})$$

en admet une et réciproquement. Mais cette dernière peut s'écrire

$$(\alpha\xi + \alpha_1)^2 + \alpha\alpha_2 - \alpha_1^2 \equiv (\mathfrak{p}).$$

Résoudre (1) cela revient à résoudre les deux congruences

(2_a) $$\sigma^2 + \alpha^* \equiv 0 \ (\mathfrak{p})$$

(2_b) $$\alpha\xi + \alpha_1 \equiv \sigma \ (\mathfrak{p}).$$

La dernière admet toujours une racine lorsqu'on connait σ, il ne reste plus qu'à considérer ($2a$).

Si α ou α_2 était divisible par $\mathfrak{p}$ (1), se réduisait à une congruence

linéaire. D'autre part si α_1 est divisible par $\mathfrak{p}$, nous sommes ramenés à

(3) $$\alpha_1\xi^2 + \alpha_2 \equiv 0\ (\mathfrak{p}).$$

et cette congruence admet les racines, s'il en est ainsi de

(4) $$\alpha_1^{n(\mathfrak{p})-2}(\alpha_1\xi^2 + \alpha_2) \equiv 0\ (\mathfrak{p}).$$

Mais en vertu du théorème de Fermat, cela revient à

$$\xi^2 + \alpha^* \equiv 0\ (\mathfrak{p}).$$

La résolution d'une congruence du second degré se ramène toujours à l'étude d'une équation de la forme

$$\xi^2 - \alpha \equiv 0\ (\mathfrak{p}).$$

Nous supposerons d'abord que l'idéal $\mathfrak{p}$ ne divise pas l'idéal (2). La congruence $\xi \equiv 0$, admet une solution que nous considérerons comme une solution double, il ne nous reste plus que le cas où (α) est premier avec $\mathfrak{p}$.

Si π est une racine primitive de $\mathfrak{p}$ il y a un exposant a tel que

$$\alpha \equiv \pi^a\ (\mathfrak{p}).$$

De là, il résulte que la congruence admet une solution lorsque a est pair. Nous allons montrer que la condition nécessaire et suffisante pour qu'il en soit ainsi, est que

$$\alpha^{\frac{n(\mathfrak{p})-1}{2}} \equiv (\pi^a)^{\frac{n(\mathfrak{p})-1}{2}} \equiv +1\ (\mathfrak{p}),$$

comme il résultera du théorème suivant :

Théorème. — La congruence quadratique $\xi^2 \equiv \alpha\ (\mathfrak{p})$ suivant un module premier $\mathfrak{p}$ qui ne divise pas (2) admet deux racines incongrues pour α premier avec $\mathfrak{p}$, si

$$\alpha^{\frac{n(\mathfrak{p})-1}{2}} \equiv +1\ (\mathfrak{p})$$

et dans ce cas seulement. Lorsque la congruence admet des racines on dit que α est resté quadratique de $\mathfrak{p}$, dans le cas contraire α est

dit non reste quadratique de $\mathfrak{p}$. Dans le premier cas, nous poserons

$$\left(\frac{\alpha}{\mathfrak{p}}\right) = 1,$$

dans le second

$$\left(\frac{\alpha}{\mathfrak{p}}\right) = -1.$$

D'après le théorème de Fermat généralisé puisque α est premier avec α

$$\alpha^{n(\mathfrak{p})-1} \equiv 1 \ (\mathfrak{p})$$

ou

$$\alpha^{n(\mathfrak{p})-1} - 1 \equiv 0 \ (\mathfrak{p})$$

ce qui donne

$$\left(\alpha^{\frac{n(\mathfrak{p})-1}{2}} + 1\right)\left(\alpha^{\frac{n(\mathfrak{p})-1}{2}} - 1\right) = 0,$$

$\mathfrak{p}$ premier avec α ne peut diviser ces deux facteurs à la fois, que s'il divise $2\alpha^{\frac{n(\mathfrak{p})-1}{2}}$ et par suite 2. L'une des deux congruences

$$\alpha^{\frac{n(\mathfrak{p})-1}{2}} \equiv 1 \ (\mathfrak{p})$$

$$\alpha^{\frac{n(\mathfrak{p})-1}{2}} \equiv -1 \ (\mathfrak{p}),$$

est satisfaite et l'une d'elles seulement, si $(\mathfrak{p})$ ne divise pas 2.

Dans le cas où c'est la première, on a, en posant $\alpha = \pi^a \ (\mathfrak{p})$

$$\alpha^{\frac{n(\mathfrak{p})-1}{2}} \equiv (\pi^a)^{\frac{n(\mathfrak{p})-1}{1}} \equiv 1 \ (\mathfrak{p}),$$

il faut que a soit pair, et l'on a $\left(\frac{\alpha}{\mathfrak{p}}\right) = 1$. Si c'est la seconde congruence qui est vérifiée

$$\alpha^{\frac{n(\mathfrak{p})-1}{2}} \equiv (\pi^a)^{\frac{n(\mathfrak{p})-1}{1}} \equiv -1 \ (\mathfrak{p}),$$

a est certainement impair et par suite $\left(\frac{\alpha}{\mathfrak{p}}\right) = -1$.

α est donc reste quadratique ou non reste suivant $\mathfrak{p}$, suivant que

$$\alpha^{\frac{n(\mathfrak{p})-1}{2}} \equiv \pm 1 \ (\mathfrak{p}),$$

ou encore

$$\alpha^{\frac{n(\mathfrak{p})-1}{2}} \equiv \left(\frac{\alpha}{\mathfrak{p}}\right) (\mathfrak{p}).$$

On a de plus le théorème.

Théorème. — Il y a $\frac{n(\mathfrak{p})-1}{2}$ restes quadratiques incongrus suivant un idéal premier $\mathfrak{p}$, qui ne divise pas 2 et autant de non restes.

Cela résulte de ce fait que les $n(\mathfrak{p}) - 1$ puissances π, π^2 ... d'une racine primitive forment un système complet de restes suivant $\mathfrak{p}$.

Théorème. — Soient α et β deux nombres entiers du corps $k(\sqrt{m})$ qui ne sont pas divisibles par l'idéal $\mathfrak{p}$, on a

$$\left(\frac{\alpha\beta}{\mathfrak{p}}\right) = \left(\frac{\alpha}{\mathfrak{p}}\right)\left(\frac{\beta}{\mathfrak{p}}\right).$$

Démonstration : On a

$$\left(\frac{\alpha}{\mathfrak{p}}\right) = \alpha^{\frac{n(\mathfrak{p})-1}{2}}, \quad \left(\frac{\beta}{\mathfrak{p}}\right) = \beta^{\frac{n(\mathfrak{p})-1}{2}} \ (\mathfrak{p}),$$

par suite

$$\left(\frac{\alpha}{\mathfrak{p}}\right)\left(\frac{\beta}{\mathfrak{p}}\right) = (\alpha\beta)^{\frac{n(\mathfrak{p})-1}{2}} \equiv \left(\frac{\alpha\beta}{\mathfrak{p}}\right) (\mathfrak{p}),$$

c'est-à-dire

$$\left(\frac{\alpha}{\mathfrak{p}}\right)\left(\frac{\beta}{\mathfrak{p}}\right) = \left(\frac{\alpha\beta}{\mathfrak{p}}\right).$$

Il est facile de traiter directement le cas de $\mathfrak{p}$ diviseur de (2). Si dans le corps $k(\sqrt{m})$ l'idéal (2) se décompose en $\mathfrak{p}$, $\mathfrak{p}'$, on a $n(\mathfrak{p}) = 2$.

$\Phi(\mathfrak{p}) = 1$ et comme α est premier avec (2) il est reste quadratique suivant $\mathfrak{p}$, car on a alors

$$\alpha \equiv 1 \ (\mathfrak{p}).$$

Mais si (2) est lui-même un idéal premier, ce qui arrive pour $m \equiv 5 \ (8)$ les nombres du corps incongrus suivant (2) sont 1, ω, $1+\omega$, α est encore reste quadratique suivant $\mathfrak{p}$, car la congruence quadratique admet des racines pour $\alpha \equiv 1, \omega, 1+\omega$ ainsi qu'on le voit en calculant directement les racines.

Le symbole $\left(\frac{\alpha}{\mathfrak{p}}\right)$ ne peut prendre que les deux valeurs $+1$ et -1 lorsque α est premier avec $\mathfrak{p}$ et que $\mathfrak{p}$ ne divise pas (2). Nous dirons encore que c'est le symbole de Legendre, car il est la généralisation de ce symbole dans le domaine des nombres algébriques.

Considérons maintenant la congruence

$$\xi^2 - \alpha \equiv 0 \ (\mathfrak{p}^k)$$

α premier avec $\mathfrak{p}$. Nous distinguerons deux cas : 1° $\mathfrak{p}$ est premier avec 2 ; 2° $\mathfrak{p}$ divise 2.

Dans le premier cas on voit que la congruence ne peut admettre de racine que s'il en est ainsi de $\xi^2 - \alpha \equiv 0 \ (\mathfrak{p})$, c'est-à-dire si $\left(\frac{\alpha}{\mathfrak{p}}\right) = 1$.

Mais supposons cette condition remplie, et désignons par λ une racine quelconque de cette congruence, λ étant premier avec $\mathfrak{p}$, il y a une infinité de racines de la congruence comprises dans la formule

$$\xi = \lambda + p\rho$$

ρ prenant toutes les valeurs entières du corps.

Parmi ces nombres il y aura une racine de

$$\xi^2 - \alpha \equiv 0 \ (\mathfrak{p}^k)$$

si cette racine existe.

Posons d'abord $k = 2$ et admettons que p n'est pas divisible par $\mathfrak{p}^2$ il reste à déterminer ρ de telle sorte que

$$(\lambda + p\rho)^2 - \alpha \equiv 0 \ (\mathfrak{p}^2)$$

$p^2 \equiv 0\ (\mathfrak{p}^2)$ on doit avoir

$$2p\lambda\rho + \lambda^2 - \alpha \equiv 0\ (\mathfrak{p}^2)$$

si $\lambda^2 - \alpha$ était divisible par $\mathfrak{p}^2$ il suffirait de faire $\rho \equiv 0\ (\mathfrak{p})$. Ce cas étant exclu, pourra-t-on déterminer ρ entier de façon que

$$2p\lambda\rho + \lambda^2 - \alpha \equiv (\mathfrak{p}^2)$$

et cela n'est possible que si le plus grand commun diviseur de $2p\lambda$ et de $\mathfrak{p}^2$, c'est-à-dire l'idéal premier $\mathfrak{p}$ divise aussi $\lambda^2 - \alpha$, ce qui est le cas.

ρ étant ainsi déterminé

$$\xi = \lambda + p\rho$$

sera une solution de

$$\xi^2 - \alpha \equiv 0\ (\mathfrak{p}^2).$$

On voit facilement que l'on aura de même une solution de

$$\xi^2 \equiv \alpha\ (\mathfrak{p}^3)$$

on arrivera enfin au

Théorème. — Si $\mathfrak{p}$ est un idéal premier du corps $k(\sqrt{m})$ qui ne divise pas 2 et si α est un entier du corps qui n'est pas divisible par $\mathfrak{p}$. La congruence

$$\xi^2 \equiv \alpha\ (\mathfrak{p}^h)$$

admet des solutions ou n'en admet pas suivant que

$$\left(\frac{\alpha}{\mathfrak{p}}\right) = 1 \quad \text{ou} \quad \left(\frac{\alpha}{\mathfrak{p}}\right) = -1.$$

Lorsque $\mathfrak{p}^2$ divise le nombre rationnel p, c'est-à-dire si p divise le discriminant, il faut modifier quelque peu l'étude de la congruence.

La congruence

$$\xi^2 - \alpha \equiv 0\ (\mathfrak{p}^h)$$

n'admet des racines que si

$$\xi^2 - \alpha \equiv 0\ (\mathfrak{p}^2)$$

en a aussi.

On peut résoudre le cas de $\mathfrak{p}$ diviseur de 2 comme le précédent et on voit que :

Théorème. — Si $\mathfrak{p}$ est un idéal premier du corps qui divise 2 et si α est premier avec $\mathfrak{p}$ la congruence

$$\xi^2 - \alpha \equiv 0 \ (\mathfrak{p}^k)$$

admet des racines pour tout exposant k en même temps que

(I) $$\xi^2 - \alpha \equiv 0 \ (\mathfrak{p}^6)$$

si $\mathfrak{p}$ est un idéal du premier degré, et en même temps que

(II) $$\xi^2 - \alpha \equiv 0 \ (\mathfrak{p}^3)$$

si $\mathfrak{p}$ est un idéal du second degré.

Les congruences I et II se résolvent par une discussion de tous les cas particuliers qui peuvent se présenter, on trouve, il faut que pour les 2 cas, soit $\alpha \equiv 1 \ (\mathfrak{p}^6)$ soit $\alpha \equiv 1 \ (8)$.

On obtient toujours les quatre racines incongrues ± 1, ± 3.

Nous engageons le lecteur à traiter quelques cas particuliers $k(\sqrt{-1})$, $k(\sqrt{-2})$, $k(\sqrt{2})$ et à faire les calculs numériques.

22. Les unités du corps quadratique. — On appelle unités du corps tous les entiers qui divisent ± 1 ou ce qui revient au même, ceux dont la norme $= \pm 1$. Nous allons tout d'abord démontrer l'existence de ces unités, et pour cela nous nous appuierons sur le théorème de Minkowski.

Théorème I. — Un corps imaginaire quelconque ne possède d'autres unités que ± 1, de plus le corps $k(\sqrt{-1})$ a en outre les unités $\pm \sqrt{-1}$ et le corps $k(\sqrt{-3})$ a les unités $\pm \dfrac{1 \pm \sqrt{-3}}{2}$.

Démonstration : Considérons d'abord le corps $k\sqrt{-1}$, $x + y\sqrt{-1}$ est une unité si sa norme $= \pm 1$

$$n(x + \sqrt{-1}\,y) = x^2 + y^2 = \pm 1$$
$$x^2 + y^2 = -1$$

ne peut être satisfaite pour aucune valeur réelle de x et de y tandis que

$$x^2 + y^2 = 1$$

admet des solutions

$$\begin{array}{lll} 1. & x = 1, & y = 0 \\ 2. & x = -1, & y = 0 \\ 3. & x = 0, & y = 1 \\ 4. & x = 0, & y = -1 \end{array}$$

et n'en admet pas d'autre.

Ces unités du corps sont donc

$$+1, \quad -1, \quad +\sqrt{-1}, \quad -\sqrt{-1}.$$

Ce sont les racines carrées de ± 1, aussi dit on que ce sont des racines de l'unité.

Deuxièmement dans le corps $k(\sqrt{-3})$ le nombre entier

$$x + \frac{1+\sqrt{-3}}{2}y$$

est une unité si

$$\left(x + \frac{1}{2}y\right)^2 + \frac{3}{4}y^2 = \pm 1$$

ce qui donne

$$x^2 + xy + y^2 = +1$$

dont les solutions sont :

$$\begin{array}{lll} 1.\ x = 1 \quad y = 0, & 3.\ x = 1 \quad y = -1, & 5.\ x = 0\ y = 1 \\ 2.\ x = -1\ y = 0, & 4.\ x = -1\ y = 1, & 6.\ x = 0\ y = -1. \end{array}$$

On a alors comme unités du corps

$$\pm 1, \pm \omega = \pm \frac{1+\sqrt{-3}}{2}, \pm \omega' = \pm \frac{1-\sqrt{-3}}{2}$$

sous ces nombres sont des racines cubiques de l'unité. Pour tout autre corps imaginaire $k(\sqrt{m})$ un nombre entier est de la forme

$$x + \sqrt{m}\,y$$

dans le cas $m \not\equiv 1$ (4) ou

$$x + \frac{1+\sqrt{m}}{2}$$

dans le cas $m \equiv 1$ (4) le nombre est une unité si

$$x^2 - my^2 = \pm 1$$

dans le premier cas

$$\left(x + \frac{1}{2}y\right)^2 - \frac{m}{4}y^2 = \pm 1$$

dans le second cas. Soit $m = -|m|$ nous aurons

$$x^2 + |m| y^2 = \pm 1$$

$$\left(x + \frac{1}{2}y\right)^2 + \left(\frac{m}{4}\right)y^2 = \pm 1.$$

On ne peut considérer que le signe $+$, d'ailleurs dans le premier cas $|m| \geqq 3$, dans le second cas $|m| \geqq 7$, on ne peut avoir d'autres solutions que

$$x = +1, \quad y = 0$$

$$x = -1, \quad y = 0,$$

car dès que $|y| \geqq 1$, le premier nombre est > 1 pour toutes les valeurs réelles de x. ± 1 sont dans les seuls valeurs unités du corps imaginaire le plus général.

Théorème 2. — Dans chaque corps réel $k(\sqrt{m})$ il y a une infinité d'unités différentes de ± 1 et parmi celles-là, il y a une unité fondamentale ε telle que $|\varepsilon| > 1$, et que toute unité puisse être mise sous la forme $\pm \varepsilon^e$, où e est un exposant entier rationnel quelconque positif ou négatif.

Nous ferons la démonstration en deux parties : la première consistera à démontrer l'existence d'unités différentes de ± 1 ; la seconde à démontrer l'existence de l'unité fondamenlale ε, ayant la propriété énoncée.

La première partie consiste à démontrer que les équations

$$1. \quad x^2 - my^2 = \pm 1, \qquad (m \not\equiv 1), (4)$$

$$2. \quad \left(x + \frac{1}{2}y\right)^2 - \frac{m}{4}y^2 = \pm 1, \qquad (m \equiv 1), (4),$$

admettent des solutions entières pour toute valeur positive entière de m, où qu'elles en admettent tout au moins si l'on prend le second membre avec le signe $+$.

Soit d le discriminant du corps, et soit ω, ω', avec la signification ordinaire $+\sqrt{m}$ pour $m \not\equiv 1$, (4), $\frac{1 + \sqrt{m}}{2}$ pour $m \equiv 1$ (4)

$$3. \quad f = x - \omega y$$

$$4. \quad f' = x - \omega' y,$$

sont deux formes linéaires et homogènes à coefficients réels et dont le déterminant

$$\begin{vmatrix} 1 & -\omega \\ 1 & -\omega' \end{vmatrix} = \omega - \omega' = \sqrt{d}$$

est réel et positif, de plus

$$ff' = x^2 - my^2 \quad \text{ou} \quad x^2 + mxy + \frac{1-m}{4} y^2.$$

Soient $\varkappa$, $\varkappa_1$ deux nombres réels quelconques dont le produit est $\sqrt{d}$, on pourra trouver deux nombres entiers rationnels x et y, qui ne sont pas tous deux nuls, tels que

$$5. \quad |f| = |x - \omega y| \leqq \varkappa$$
$$6. \quad |f| = |x - \omega' y| \leqq \varkappa_1.$$

On déterminera d'abord deux nombres entiers et rationnels différents de zéro x_1, y_1, tels que pour certaines valeurs quelconques des $\varkappa$ par exemple.

$$\varkappa = 1, \quad \varkappa_1 = \sqrt{d},$$

on ait

$$|x_1 - \omega y_1| \leqq \varkappa, \qquad |x_1 - \omega' y_1| \leqq \varkappa_1,$$

et l'on fera

$$\alpha_1 = x_1 - \omega y_1.$$

Ensuite on déterminera x_2, y_2, entiers rationnels tels que

$$|x_2 - \omega y_2| \leqq \left|\frac{\alpha_1}{2}\right|$$

$$|x_2 - \omega' y_2| \leqq \frac{2\sqrt{d}}{|\alpha_1|}$$

et l'on fera

$$\alpha_2 = x_2 - \omega y_2,$$

x_2, y_2 sont différents de x_1, y_1, et α_2 diffère de α_1. On continuera ainsi, et on formera la suite.

$$7. \quad \alpha_1, \alpha_2, \alpha_3, \ldots$$

telle que

$$8. \quad |\alpha_1| > |\alpha_2| > |\alpha_3| \cdots$$

et alors les idéaux (α_1), (α_2), (α_3) ... forment une suite indéfinie d'idéaux dont les normes sont en valeur absolue plus petite que $\sqrt{d}$. On a d'ailleurs démontré précédemment qu'il ne peut y avoir qu'un nombre fini d'idéaux dont la norme est inférieure à un nombre fini donné. Il faudra donc que dans la suite illimitée, on ait un nombre infini de fois des idéaux égaux.

Soit par exemple

$$(\alpha_1) = (\alpha_r),$$

c'est donc que $\frac{\alpha_1}{\alpha_r}$ et $\frac{\alpha_r}{\alpha_1}$ représentant l'un et l'autre un nombre entier (non rationnel) des corps, soit

$$\alpha_1 = \varepsilon_r \alpha_r,$$

où ε_1 est une *unité* du corps différente de ± 1. Comme de plus, on a en les valeurs absolues, la condition $|\alpha_1| > |\alpha_r|$ il faut nécessairement que $|\varepsilon_r| > 1$.

D'ailleurs dans un corps réel, la valeur absolue d'un $|\varepsilon_r|$ n'est égale à 1, que si $\varepsilon_r = \pm 1$. On a alors d'une façon générale

$$|\alpha| = |\alpha'| \qquad \text{ou} \qquad |x + \omega y| = |x + \omega' y|$$

et alors

$$y = 0, \qquad \alpha = \pm \alpha'.$$

Cette conclusion nous montre d'ailleurs que l'équation

$$x^2 - my^2 = 1$$

ou

$$x^2 + xy + \frac{1 - m}{4} y^2 = 1,$$

à laquelle on donne le nom d'équation de Pell. (1), admet tou-

---

(1) Voir A. Konen, sur l'historique de l'équation $t^2 - Du^2 = 1$. Leipzig 1901. Fermat a sans doute déjà résolu cette équation dont les solutions faites antérieurement étaient sans doute perdues. (Lettre de Fermat à Frénicle 1657). Œuvres de Fermat, t. II, p. 333.

Voir Gauss, *Disq. arithm.* V. Art. 198, 200, 201, 202. — Legendre. Théorie des nombres. — Schubert. *Vorles.*, t. II. Leipzig 1906.

jours une solution entière. Ce que nous venons de dire ne permet pas de reconnaître s'il en est ainsi des équations

$$x^2 - my^2 = -1, \quad x^2 + xy + \frac{1-m}{4} y^2 = -1.$$

Nous montrerons plus loin (N° 24) qu'il y en a une infinité de valeurs de m pour lesquelles ces dernières équations ne peuvent admettre des solutions entières et rationnelles. Par contre, on a trouvé dans certains cas particuliers les valeurs de m pour lesquelles elles admettent des solutions. (Voir n° 23 et 32).

Nous allons voir que dans un corps réel que toutes les puissances positives ou négatives d'une unité ε, nous donnent une infinité d'unités différentes.

Si ε est une unité

$$n(\varepsilon^a) = [n(\varepsilon)]^a = (\pm 1)^a$$

ε^a est une unité. Soit

$$a_1 \neq a \quad \text{et} \quad \varepsilon \neq 1$$

ε^a et ε^{a_1} sont différents.

Si l'on pose

$$\varepsilon^a = u + v\omega \quad x = u \quad y = v,$$

forment une solution de l'une des équations (1) ou (2) soit pour le signe $+$, soit pour le signe $-$ du second membre.

A chaque unité ε dont la valeur absolue est < 1 correspond une unité $\frac{1}{\varepsilon}$ telle $\left|\frac{1}{\varepsilon}\right| > 1$.

Si l'on admet que l'équation

$$x^2 - my^2 = -1$$

ou encore

$$x^2 + xy + \frac{1-m}{4} y^2 = -1,$$

possède une solution, c'est-à-dire lorsque le corps $k(\sqrt{m})$ possède une unité ε_1 telle que $n(\varepsilon_1) = -1$, les puissances impaires de cette unité ε_1^3, e_1^5 ... donnent une infinité d'autres solutions

de cette équation, car $n(\varepsilon_s^{2a+1}) = -1$. Les puissances paires ε_s^2, ε_s^4 ... donnent une infinité de solutions distinctes de

$$x^2 - my^2 = +1 \qquad x^2 + xy + \frac{1-m}{4} y^2 = +1$$

car $n(\varepsilon_s^{2a}) = +1$.

On peut ordonner les unités dont la valeur absolue > 1, suivant la grandeur de leurs valeurs absolues, car si η et η_1 sont de ces unités, on ne peut avoir $|\eta_1| = |\eta_2|$, c'est-à-dire $\eta_1 = \pm \eta_2$ les deux unités ne seraient donc pas réellement distinctes, il faut donc $\eta_1 > \eta_2$ ou $\eta_1 < \eta_2$.

On peut obtenir cette remarque par la considération directe des équations (1) et (2) qui déterminent les unités.

Car si $x_1 y_1$ et $x_2 y_2$ représentent deux solutions entières, soit de

$$x^2 - my^2 = 1, \quad \text{soit de} \quad x^2 - my^2 = +1,$$
$$y_1 \geqslant y_2 \quad \text{entraîne} \quad x_1 \geqslant x_2 \quad \text{et} \quad y_1 < y_2, \quad x_1 < x_2.$$

Si de plus

$$x_1^2 - my_1^2 = +1, \qquad x_2^2 - my_2^2 = -1,$$
$$y_1 \geqslant y_2 \quad \text{donne} \quad x_1 > x_2 \quad \text{et} \quad y_1 < y_2 \quad \text{donne} \quad x_1 < x_2.$$

Soit

$$m \not\equiv 1 \ (4) \qquad \text{et} \qquad \eta_i = x_i + y_i \sqrt{m}$$

une unité du corps avec $x_i > 0$, alors $|\eta_i| > 1$, quand y_i est positif. Si maintenant

$$\eta_1 = x_1 + y_1 \sqrt{m}, \qquad \eta_2 = x_2 + y_2 \sqrt{m}$$

sont deux unités de cette nature $y_1 > y_2$ entraîne $|\eta_1| > (\eta_2)$ et réciproquement.

On obtient le même résultat dans le cas de $m \equiv 1 \ (4)$ en écrivant

$$\eta_i = \left(x_i + \frac{y_i}{2}\right) + \frac{y_i}{2} \sqrt{m}$$

et en remplacement dans le raisonnement précédent x_i par

$$x_i + \frac{y_i}{2}.$$

Résolvant maintenant les questions

$$x^2 - my^2 = \pm 1 \quad \text{ou} \quad x^2 + xy + \frac{1-m}{4}y^2 = \pm 1,$$

pour le signe + du second membre et lorsque cela est possible pour le signe —, et ordonnons les unités η telles que $|\eta| > 1$, et dont l'y est positif suivant les valeurs croissantes des y, ces unités seront elles-mêmes rangées par ordre de grandeur croissante

$$|\varepsilon| < \dots < |\eta_1| < |\eta_2| \dots$$

Soit alors $|\varepsilon|$ la plus petite de ces valeurs absolues, ε signera à un signe près une unité bien déterminée du corps, je *dis que ε est une unité fondamentale.*

En effet soit η une unité quelconque et supposons $|\eta| > 1$, on peut déterminer un entier positif e tel que

$$|\varepsilon^e| \leq \eta < |\varepsilon^{e+1}|$$

c'est-à-dire

$$1 \leq \left|\frac{\eta}{\varepsilon^e}\right| < |\varepsilon|.$$

Mais comme $\left|\frac{\eta}{\varepsilon^e}\right|$ est une unité, et il n'y a pas d'unité dont la valeur absolue est comprise entre 1 et $|\varepsilon|$ il faut que

$$\left|\frac{\eta}{\varepsilon^e}\right| = 1,$$

c'est-à-dire

$$\eta = \pm \varepsilon^e,$$

on montrerait de même qu'une unité dont la valeur absolue < 1 est égale à $\pm \frac{1}{\varepsilon^{e_1}}$. Nous avons donc montré que les unités du corps se mettent sous la forme $\pm \varepsilon^e$, où e prend toutes les valeurs entières et rationnelles.

Dans le cas où le corps admet les unités de norme -1, il faut que l'unité fondamentale ait une norme $= -1$, car si sa norme était égale à $+1$, toutes les puissances de cette unité auraient une norme $= +1$. Soit

$$\varepsilon = x + y\omega$$

avec y positif, y et x, ou y et $x + \frac{y}{2}$ sont les plus petites solutions positives des équations

$$x^2 - my^2 = \pm 1$$

ou

$$x^2 + xy + \frac{1 - m}{4} y^2 = \pm 1,$$

et cela pour le signe + ou le signe — du second membre suivant que

$$n(\varepsilon) = + 1$$

ou

$$n(\varepsilon) = - 1.$$

On pourra donc déterminer l'unité fondamentale par un nombre limité d'opérations, car on peut obtenir les solutions des opérations (1) ou (2) soit par des essais, soit par un développement en fraction continue.

Supposons que l'on ne sache pas si la norme de l'unité fondamentale est égale à — 1. On cherchera η de norme + 1 avec la condition $|\eta| > 1$ et telle que $|\eta|$ soit la plus petite solution en valeur absolue, et cela en déterminant la plus petite solution en valeur absolue de

$$x^2 - my^2 = + 1$$

respectivement de

$$x^2 + xy + \frac{1 - m}{4} y^2 = + 1.$$

Puis on posera

$$\eta = \pm \varepsilon^2 = \pm (x + y\omega)^2.$$

Suivant que cette équation admet des solutions entières x et y, ou non, c'est ε ou η qui est l'unité fondamentale.

On peut résumer ainsi les théorèmes sur les unités :

Dans un corps quadratique les unités peuvent être mises sous la forme unique

$$\rho\varepsilon^r,$$

ε étant l'unité fondamentale et ζ une racine de l'unité appartenant au corps, et où $\varepsilon = +1$ pour tous les corps imaginaires et où $\varepsilon \neq 1$, pour tous les corps réels.

1[er] *Exemple.* — $k(\sqrt{3})$. $2 + \sqrt{3}$ est une unité fondamentale car l'équation

$$x^2 - 3y^2 = \pm 1$$

n'admet de racine que pour le signe $+$ au second membre

$$x = 2, \quad y = 1$$

formant la solution la plus petite en valeur absolue. On a d'autres unités par exemple.

$$\eta_1 = \varepsilon^2 = 7 + 4\sqrt{3}, \quad \eta_2 = \varepsilon^3 = 26 + 15\sqrt{3},$$

etc.

$$\varepsilon' = \frac{1}{\varepsilon} = 2 - \sqrt{3}$$

$$\varepsilon'^2 = 7 - 4\sqrt{3}, \quad \varepsilon'^3 = 26 - 15\sqrt{3}$$

etc. Toutes les normes sont égales à $+1$.

2[e] *Exemple.* — $k(\sqrt{14})$

$$x = 15, \quad y = 4$$

est la plus petite solution de

$$x^2 - 14y^2 = +1$$

$$\varepsilon = 15 + 4\sqrt{14}$$

est l'unité fondamentale car

$$x^2 - 14y^2 = -1$$

n'admet pas de solution. On a d'autres unités par exemple

$$\varepsilon^2 = 449 + 120\sqrt{14}, \quad \varepsilon^3 = 13455 + 3596\sqrt{14}$$

$$\varepsilon' = \frac{1}{\varepsilon} = 15 - 4\sqrt{14}$$

$$\varepsilon'^2 = 449 - 120\sqrt{14}, \quad \varepsilon'^3 = 13455 - 3596\sqrt{14}.$$

3e *Exemple.* — $k(\sqrt{5})$

$$x^2 + xy - y^2 = -1$$

admet

$$x = 0, \quad y = 1$$

on a

$$\varepsilon = \omega, \quad n(\varepsilon) = -1$$
$$\varepsilon^2 = 1 + \omega, \quad n(\varepsilon^2) = +1$$
$$\varepsilon^3 = 1 + 2\omega, \quad n(\varepsilon^3) = -1$$
$$\varepsilon' = \frac{1}{\varepsilon} = \omega'.$$

On verra plus loin que dans le cas de $m \equiv (1)\, 4$, que les deux équations

$$x^2 + xy + \frac{1-m}{4} y^2 = \pm 1$$
$$x_1^2 - my_1^2 = \pm 1,$$

admettent simultanément des racines pour le signe — au second membre. (Voir n° 33),

23. Les corps dont le nombre des classes est impair. — *Théorème* (1). Tout nombre entier ou fractionnaire du corps $k(\sqrt{m})$, dont la norme égale $+1$, peut-être représenté par le quotient de deux nombres entiers conjugués du corps, c'est-à-dire qu'il peut être mis sous la forme $\frac{\gamma}{\gamma'}$.

Démonstration : On peut toujours écrire pour tout nombre entier ou fractionnaire

$$\alpha = \frac{a}{c} + \frac{b}{c}\omega$$

où a, b, c sont des entiers rationnels. Mais comme $n(\alpha) = 1$, a et b sont premiers entre eux, si l'on admet à priori que a, b, c n'ont pas de diviseur commun.

Nous distinguerons deux cas :

$$m \equiv 1 \quad \text{et} \quad m \not\equiv 1\ (4).$$

(1) Hilbert. — *Zahlb.* Chap. XV, § 54.

1er *Cas.* — $m \not\equiv 1\ (4)$, alors $\omega = \sqrt{m}$, et posons

$$(1) \qquad \alpha = \frac{1}{c}(a + b\omega) = \frac{x + y\omega}{x + y\omega'}.$$

Nous aurons pour calculer x et y, les deux équations linéaires.

$$(2) \qquad \left(\frac{a}{c} - 1\right) x - \frac{b}{c} m y = 0$$

$$(3) \qquad \frac{b}{c} x - \left(\frac{a}{c} + 1\right) y = 0.$$

Ces équations admettront pour x et y deux solutions entières et rationnelles différentes de o, si leur déterminant $\Delta = 0$

$$(4) \qquad \Delta = -\frac{a^2}{c^2} + 1 + \frac{b^2}{c^2} m = 1 - n(\alpha) = 0,$$

on pourra prendre

$$(5) \qquad x = \frac{1}{t}(a + c), \qquad y = \frac{1}{t} b$$

si t est un facteur commun à $a + c$ et à b.

2e *Cas.* $m \equiv 1\ (4)$

$$\omega = \frac{1 + \sqrt{m}}{2} \qquad \omega' = \frac{1 - \sqrt{m}}{2}.$$

Soit encore

$$\alpha = \frac{1}{c}(a + b\omega)$$

et posons

$$(1) \qquad \frac{a}{c} + \frac{b}{c}\omega = \frac{x + y\omega}{x + y\omega'},$$

x et y satisferont aux deux équations linéaires

$$(2) \qquad \left(\frac{a}{c} - 1\right) x + \left(\frac{a}{c} + \frac{b}{c}\frac{1 - m}{4}\right) y = 0$$

$$(3) \qquad \frac{b}{c} x - \left(\frac{a}{c} + 1\right) y = 0.$$

ces deux équations admettent encore un système de solutions entières et rationnelles si leur déterminant est nul, et on a en effet

$$\Delta = -\frac{a^2}{c^2} + 1 - \frac{ab}{c^2} - \frac{b^2}{c^2}\,\frac{1-m}{4} = 1 - n(\gamma) = 0$$

d'après l'hypothèse.

On pourra donc poser comme dans le cas précédent.

(5) $$x = \frac{1}{t}(a + c), \quad y = \frac{1}{t}\,b.$$

Dans les deux cas le nombre j à la forme suivante

$$j = \frac{1}{t}[a + c + b\omega] = \frac{c}{t}(1 + \alpha).$$

Remarque : On peut en partant de la dernière équation, démontrer ce théorème plus brièvement.

Si en particulier α est un entier du corps, c'est-à-dire une unité, on peut prendre pour γ la valeur $1 + \varepsilon$.

Voici une conséquence remarquable de ce théorème.

Théorème (¹). — Lorsque le discriminant d'un corps réel $k(\sqrt{m})$ ne contient qu'un seul nombre premier, la norme de l'unité fondamentale est égale à -1.

Démonstration : L'hypothèse exige que $m = 2$, ou que m soit un nombre premier de la forme $p \equiv 1 \ (4)$.

Soit ε l'unité fondamentale du corps. Admettons que

$$n(\varepsilon) = +1,$$

d'après ce que nous venons de dire il existe un nombre entier γ du corps tel que $\varepsilon = \frac{\gamma}{\gamma'}$. γ est un nombre entier pour lequel on a l'égalité idéale $(\gamma) = (\gamma')$ ou $(\gamma) = (\gamma)'$.

Tout idéal du corps contenu dans (γ) doit aussi être contenu dans (γ'). Mais comme le discriminant du corps ne contient qu'un nombre premier, le seul idéal ambige du corps qui est égal à son conjugué est l'idéal $\sqrt{m}$ (même pour $m = 2$), et le nombre γ ne

(¹) Hilbert. — *Zahlb.* Chap. XVII, § 68. P. Lejeune Dirichlet a démontré ce théorème d'une toute autre manière. Voir ses œuvres T. I, p. 224.

peut contenir d'autre facteur que $\sqrt{m}$ à part des facteurs entiers rationnels ou des facteurs unités. C'est-à-dire que

$$(\gamma) = (a) \quad \text{ou} \quad \gamma = \eta a$$

ou

$$(\gamma) = (\sqrt{m}) \quad \text{ou} \quad \gamma = \eta \sqrt{m}$$

où η est unité dn corps $\neq$ 1. On a dans les deux cas

$$\varepsilon = \frac{\eta \sqrt{m}}{-\eta' \sqrt{m}} = \pm \eta^2$$

et par suite ε ne serait pas une unité fondamentale comme nous l'avons supposé.

Nous en déduirons un théorème qui n'est qu'un cas particulier d'un théorème fondamental beaucoup plus général que nous démontrerons plus loin.

Théorème. — Lorsque le discriminant d'un corps $k(\sqrt{m})$ ne contient qu'un nombre premier p, le nombre des classes h du corps est impair.

Démonstration : Supposons que h soit pair, il y aurait alors certainement un idéal non principal dont le carré est un idéal principal, soit

$$\mathfrak{j}^2 \sim 1, \quad \mathfrak{j}\mathfrak{j}' \sim 1$$

donnerait alors $\mathfrak{j} \sim \mathfrak{j}'$. On pourrait donc poser $\frac{\mathfrak{j}}{\mathfrak{j}'} = \alpha$ où α est un nombre entier ou fractionnaire dont la norme

$$n(\alpha) = \pm 1.$$

Si le corps est imaginaire

$$n(\alpha) = + 1,$$

pour un corps réel

$$n(\alpha) = + 1 \quad \text{ou} \quad n(\varepsilon\alpha) = + 1,$$

ε étant l'unité fondamentale car

$$n(\varepsilon) = - 1.$$

Dans le cas où

$$n(\alpha) = + 1,$$

on peut poser $\alpha = \frac{\gamma}{\gamma'}$ dans le cas où

$$n(\alpha) = -1 \quad \text{on posera} \quad \varepsilon\alpha = \frac{\gamma}{\gamma'}.$$

Dans tous les cas $\mathfrak{j}^2 \sim 1$ entraine $(\mathfrak{j}) = (\gamma\mathfrak{j})'$. Tout idéal contenu dans l'idéal $(\gamma\mathfrak{j})$ est aussi contenu dans l'idéal conjugué $(\gamma\mathfrak{j})'$, c'est-à-dire que $(\gamma\mathfrak{j})$ n'est divisible que par des idéaux ambiges et par des idéaux principaux rationnels. Le corps $k(\sqrt{-1})$ ne contient que l'idéal ambige $(1 + \sqrt{-1})$, tous les autres corps pour $m = 2$ ou $m \equiv 1$ (4) ne contiennent que l'idéal ambige $\sqrt{m}$ $(\gamma)\,\mathfrak{j} = (a)$, ou $= (a\sqrt{m})$ ou égal à $\left(a(1 + \sqrt{-1})\right)$ pour $m = -1$.

Dans tous ces cas on voit que $\mathfrak{j} \sim 1$, ce qui est contraire à l'hypothèse. Le nombre des classes h est donc impair.

24. Théorèmes complémentaires au théorème relatif à la réciprocité quadratique. — Nous allons d'abord faire certaines remarques sur quelques corps particuliers.

I. Le corps $k(\sqrt{-1})$ a déjà été étudié par Gauss dans sa théorie des restes biquadratiques.

Dans ce corps les nombres m sont encore décomposables en facteurs premiers que d'une seule manière, $h = 1$, et les propriétés du corps sont très simples. Nous allons chercher quels sont les nombres premiers rationnels qui se décomposent dans ce corps et quels sont ceux qui ne se décomposent pas.

1. Lorsqu'un nombre premier p du corps $k(\sqrt{-1})$ est égal au produit de deux idéaux $\mathfrak{p} \cdot \mathfrak{p}' = (p)$, il n'est susceptible que d'une décomposition

$$p = (x + y\sqrt{-1})(x - y\sqrt{-1})$$

c'est-à-dire

$$p = x^2 + y^2.$$

Le nombre p par hypothèse est impair, x et y ne peuvent être tous deux pairs et ne peuvent d'ailleurs avoir aucun facteur commun. On ne peut avoir $p = x^2 + y^2$ que si x est pair et y impair, c'est-à-dire que la condition *nécessaire* pour que p soit décomposable est $p \equiv 1$ (4).

2. Cette condition est d'ailleurs *suffisante*, autrement dit si p

est un nombre premier impair $\equiv 1$ (4), p est un produit de deux facteurs dans le corps k. Nous savons que dans ce cas le corps $k(\sqrt{p})$ possède une unité fondamentale ε dont la norme est -1, c'est-à-dire que l'équation

$$\left(x + \frac{y}{2}\right)^2 - \frac{p}{4}y^2 = -1,$$

et par suite la congruence

$$(2x + y)^2 + 4 \equiv 0 \ (p)$$

peuvent être satisfaites pour des valeurs entières et rationnelles de x et de y. Soit z un entier rationel tel que

(3) $$2z \equiv 1 \ (p),$$

et multiplions les deux membres de la congruence (2) par z^2, nous verrons que la congruence $(2x + y)^2 + 4 \equiv 0 \ (p)$ est possible ou impossible en même temps que $X^2 + 1 \equiv 0 \ (p)$. Soit $X = a$ une solution de $X^2 + 1 = 0 \ (p)$, nous savons d'après le n° 14, que l'idéal (p) se décompose en deux idéaux premiers

$$(p) = (p, a + \sqrt{-1})(p, a - \sqrt{-1}).$$

Ces idéaux premiers seront d'ailleurs des idéaux principaux, et l'on a

$$p = (x + \sqrt{-1}y)(x - \sqrt{-1}y).$$

Comme un nombre premier $p \equiv 3$ (4) ne se décompose pas dans $k(\sqrt{-1})$, il en résulte que la congruence $x^2 + 1 \equiv 0 \ (p)$ est impossible lorsque $p \equiv 3$ (4).

3. Le nombre 2, qui divise le discréminant $d = -4$ du corps, se décompose

$$2 = (1 + \sqrt{-1})(1 - \sqrt{-1}),$$

c'est-à-dire que

$$(2) = (1 + \sqrt{-1})^2 = (1 - \sqrt{-1})^2,$$

$1 + \sqrt{-1}$ et $1 - \sqrt{-1}$ étant des idéaux ambiges du corps.

On peut énoncer les résultats que nous venons d'obtenir sous la forme.

Théorème. — Tout nombre entier positif rationnel p de la forme $4n + 1$ peut être mis d'une manière et d'une seule sous la forme d'une somme de deux carrés [1]

$$p = x^2 + y^2.$$

Comme cas particulier, on a :

Théorème. — La congruence quadratique

$$x^2 + 1 \equiv 0 \ (p)$$

n'admet de solution que si p est de la forme $4n + 1$, où encore un nombre de la forme $x^2 + 1$ n'admet que des diviseurs de la forme $4n + 1$. [Ce théorème est généralisé plus loin].

Enfin on voit que

$$\left(\frac{-1}{p}\right) = +1 \quad \text{pour} \quad p \equiv 1 \ (4),$$

$$\left(\frac{-1}{p}\right) = -1 \quad \text{pour} \quad p \equiv 3 \ (4),$$

ce qu'on peut résumer

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}.$$

Ce résultat peut d'ailleurs être facilement démontré d'une manière élémentaire, par exemple en partant de la congruence

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \ (p).$$

Nous avons choisi la démonstration précédente, parce qu'elle est susceptible de la plus grande généralisation.

On peut encore tirer de ce dernier théorème une conclusion très importante : Si m est un entier rationnel qui contient des facteurs premiers de la forme $p \equiv 3 \ (4)$, la congruence $x^2 + 1 \equiv 0 \ (m)$, et à plus forte raison l'équation indéterminée

$$x^2 - my^2 = -1 \quad \text{ou} \quad x^2 + xy + \frac{1-m}{4} y^2 = -1$$

---

[1] Ce théorème, dû à Fermat, a été démontré d'abord par Euler.

ne peut avoir de solution, c'est-à-dire que l'unité fondamentale ε d'un corps $k(\sqrt{m})$ dont le nombre fondamental contient des facteurs premiers de la forme $p \equiv 3\ (4)$ a toujours la norme $n(\varepsilon) = +1$.

II. Le corps $k(\sqrt{2})$. — Tous les idéaux du corps sont des idéaux principaux. Voyons quels sont les nombres premiers rationels qui dans ce corps se décomposent en un produit de deux facteurs premiers du premier degré.

1. Si p est un nombre premier impair qui se décompose dans $k\sqrt{2}$, il existe deux entiers rationnels x et y qui satisfont à

$$+p = x^2 - 2y^2,$$

car si nous considérons l'unité fondamentale $\varepsilon = 1 + \sqrt{2}$, $n(\varepsilon) = -1$, et, par suite, les équations $p = x^2 - 2y^2$, $-p = x_1^2 - 2y_1^2$ sont possibles ou impossibles simultanément, car si

$$(p) = (x + y\sqrt{2})(x - y\sqrt{2})$$

de telle sorte que

$$+p = x^2 - 2y^2,$$

on a aussi

$$(p) = (x + y\sqrt{2})(1 + \sqrt{2})(x - y\sqrt{2})(1 - \sqrt{2}),$$

c'est-à-dire

$$-p = (x + 2y)^2 - 2(x + y)^2 = x_1^2 - 2y_1^2.$$

Mais l'équation $p = x^2 - 2y^2$, où p est impair, exige que x soit impair, y étant pair ou impair, ce qui nous donne la condition nécessaire $p \equiv 1\ (8)$ ou $p \equiv 7\ (8)$.

2. La condition est suffisante, c'est-à-dire que si $p \equiv 1$ ou $p \equiv 7\ (8)$, p se décompose dans le corps $k(\sqrt{2})$.

Soit $p_1 = p$ quand $p \equiv 1\ (8)$, soit $p_1 = -p$ quand $p \equiv 7\ (8)$, on a dans les deux cas $p_1 \equiv 1\ (8)$, et le corps $k(\sqrt{p_1})$ a un nombre impair de classes h, car le discriminant du corps n'admet qu'un seul facteur premier $\pm p_1$. Soient $1, \omega = \frac{1 + \sqrt{p_1}}{2}$ les nombres de base du corps $k(\sqrt{p_1})$, on a pour l'idéal (2) les décompositions

$$(2) = (2, 1 + \omega)(2, 1 + \omega') = \mathfrak{p}.\mathfrak{p}',$$

ou

$$(2) = (2, \omega)(2, \omega') = \mathfrak{p} . \mathfrak{p}'.$$

Mais, comme d'après l'hypothèse, le nombre des classes h est impair, il existe certainement un nombre impair $2g + 1$ facteur de h, pour lesquels $\mathfrak{p}^{2g+1}$, $\mathfrak{p}'^{2g+1}$ sont des idéaux principaux.

On peut donc trouver x et y entiers et rationels, tels que

$$\mathfrak{p}^{2g+1} = (x + y\omega), \qquad \mathfrak{p}'^{2g+1} = (x + y\omega')$$

et

$$\pm 2^{2g+1} = x^2 + xy + y^2 \frac{1 - p_1}{4}.$$

On tire de là

$$(2x + y)^2 - 4 . 2^{2g+1} \equiv 0 \ (p_1),$$

et par suite

$$z^2 - 2 \equiv 0 \ (p_1)$$

admet des solutions.

Soit $z = a$ une racine de cette congruence, on a

$$(p_1) = (p_1, a - \sqrt{2})(p_1, a + \sqrt{2}),$$

comme le corps $k(\sqrt{2})$ n'a qu'une classe, les deux facteurs différents de (p_1) sont des idéaux principaux, c'est-à-dire

$$(p_1) = (x + y\sqrt{2})(x - y\sqrt{2}).$$

Il en résulte que la congruence $x^2 \equiv 2 \ (p)$ n'est possible que pour $p \equiv \pm 1 \ (8)$.

3. Enfin pour le nombre 2, on a

$$(2) = (\sqrt{2})^2$$

comme l'indique le théorème général.

Nous pouvons donc énoncer :

Théorème. — La condition nécessaire et suffisante pour que

$$x^2 - 2 \equiv 0 \ (p)$$

admette des solutions est $p \equiv \pm 1 \ (8)$.

Ou encore un nombre entier de la forme $x^2 - 2$ n'admet que des diviseurs de la forme $8n \pm 1$.

Ou enfin $\left(\frac{2}{p}\right) = +1$ lorsque p est un nombre premier impair de la forme $8n \pm 1$. $\left(\frac{2}{p}\right) = \pm 1$ lorsque $p \equiv \pm 3$ (8)

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

III. — Des considérations analogues au sujet du corps $k(\sqrt{-2})$ nous donnent :

Théorème. — La congruence quadratique $x^2 + 2 \equiv 0\,(p)$ admet des solutions pour $p \equiv 1$, $p \equiv 3$ (8), et n'en admet pas pour $p \equiv 5$, $p \equiv 7$ (8), ou encore

$$\left(\frac{-2}{p}\right) = (-1)^{\frac{p-1}{2} + \frac{p^2-1}{8}}.$$

Les égalités

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}, \qquad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

sont appelées les lois complémentaires de la loi de réciprocité.

Le caractère relatif au nombre -2 suivant p se déduit d'une façon plus simple de

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

car

$$\left(\frac{-2}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{-1}{p}\right).$$

25. Le théorème de réciprocité quadratique relatif aux nombres premiers impairs. — Les développements qui précèdent vont nous permettre d'établir le « theorema fondamentale » de Gauss.

Etant donnés deux nombres premiers impairs différents, nous allons chercher la valeur de $\left(\frac{p}{q}\right)$. La solution dépend d'un fait qu'Euler a remarqué le premier (*Opusc. anal.*, I, 1783, p. 64), ce fait est le suivant. Il existe une réciprocité entre la possibilité de

$$x^2 - q \equiv 0\ (p) \quad \text{et de} \quad x^2 - p \equiv 0\ (q).$$

Legendre a découvert ce fait à nouveau, en 1785, et l'a mis sous la forme

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

Cette formule exprime, sous la forme la plus simple, la loi de réciprocité. Depuis Gauss, bien des mathématiciens s'en sont occupés. Nous suivrons, en principe, une démonstration de Kummer (2e démonst. *Abhand. der kgl. Akademie*, Berlin, 1861), voir Hilbert, *Zahlb.*, Chap. XVII, § 68-69.

Pour simplifier la démonstration, nous emploierons les notations suivantes : Soient p, q, ... des nombres premiers impairs, pp_1p_2 ... désigneront des nombres premiers $\equiv 1$ (4), qq_1q_2 ... désigneront des nombres premiers $\equiv 3$ (4).

Dans notre démonstration, nous aurons à distinguer trois cas : p, p_1, pq et q, q_1.

1er *Cas*. — Si la congruence

$$x^2 - p \equiv 0 \ (p_1)$$

est possible, c'est-à-dire si $\left(\frac{p}{p_1}\right) = +1$, p_1 dans le corps $k(\sqrt{p})$ pourra être décomposé en un produit de deux idéaux distincts du 1er degré. On aura :

$$(p_1) = (p_1, a + \omega)(p_1, a + \omega') = \mathfrak{p}\cdot\mathfrak{p}'.$$

Mais, comme le nombre h des classes du corps $k(\sqrt{p})$ est impair, le discriminant du corps n'ayant pas d'autre facteur premier que p, il y a toujours un nombre impair $h_1 = 2g + 1$, facteur de h, tel que les puissances d'exposant h_1, de $\mathfrak{p}$ et de $\mathfrak{p}'$, deviennent des idéaux principaux. Comme, de plus, la norme de l'unité fondamentale ε du corps $k(\sqrt{p}) = -1$, on peut poser :

$$p_1^{2g+1} = (x + y\omega)(x + y\omega'),$$

c'est-à-dire

$$p_1^{2g+1} = \left(x + \frac{y}{2}\right)^2 - \frac{p}{4}y^2,$$

d'où il résulte

$$(2x + y)^2 - p_1(2p_1^g)^2 \equiv 0 \ (p).$$

On en conclut, comme précédemment, que la congruence

$$z^2 - p_1 \equiv 0 \ (p),$$

ou encore

$$x^2 - p_1 \equiv 0 \ (p)$$

est possible.

Si donc $\left(\frac{p}{p_1}\right) = + 1$, on a aussi $\left(\frac{p}{p_1}\right) = + 1$.

Il en résulte de plus, que, si $\left(\frac{p}{p_1}\right) = - 1$, $\left(\frac{p_1}{p}\right) = - 1$. Car, en effet, si on avait $\left(\frac{p_1}{p}\right) = + 1$, on aurait aussi $\left(\frac{p}{p_1}\right) = + 1$, ce qui est contraire à l'hypothèse.

2e *Cas.* — Soit $x^2 - p \equiv 0 \ (q)$.

Supposons $\left(\frac{p}{q}\right) = 1$, de telle sorte que q se décompose dans le corps $k(\sqrt{p})$,

$$(q) = (q, a - b\omega)(q, a + b\omega'),$$

nous pourrons encore remarquer que le nombre des classes est impair, et que $n(\varepsilon) = - 1$, et que, par suite, on a, pour certains entiers rationiels, x et y

$$q^{2g+1} = \left(x + \frac{y}{2}\right)^2 - \frac{p}{4} y^2,$$

ou, encore, la congruence $x^2 - q \equiv 0 \ (p)$ est possible en nombres entiers. Donc $\left(\frac{p}{q}\right) = + 1$ entraîne $\left(\frac{q}{p}\right) = + 1$.

Il nous reste à montrer que $\left(\frac{q}{p}\right) = 1$ entraîne $\left(\frac{p}{q}\right) = 1$.

Si $\left(\frac{q}{p}\right) = + 1$, c'est-à-dire si $x^2 - q \equiv 0 \ (p)$ est possible, $x^2 + q \equiv 0 \ (p)$ l'est aussi, car

$$\left(\frac{-q}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{q}{p}\right) = \left(\frac{q}{p}\right),$$

ou encore, on sait qu'il existe un nombre entier rationnel z, tel que $z^2 \equiv - 1 \ (p)$; si donc on a

$$x^2 - q \equiv 0 \ (p)$$
$$(zx)^2 - z^2 q \equiv 0 \ (p),$$

en posant $X \equiv zx$, on voit que $X^2 + q \equiv 0 \ (p)$.

Comme $\left(\frac{-q}{p}\right) = +1$, p se décompose dans le corps imaginaire $k(\sqrt{-q})$, et comme $-q \equiv +1$ (4), le nombre des classes du corps $k(\sqrt{-q})$ est encore impair, et on conclut, comme dans les cas précédents, en tenant compte de ce fait, que la norme d'un nombre entier du corps $k(\sqrt{-q})$ est toujours positive, que la congruence

$$x^2 - p \equiv 0 \ (q)$$

est aussi possible.

En somme, si

$$\left(\frac{p}{q}\right) = +1, \quad \left(\frac{q}{p}\right) = +1,$$

et si

$$\left(\frac{q}{p}\right) = +1, \quad \left(\frac{p}{q}\right) = -1;$$

par conséquent, si

$$\left(\frac{p}{q}\right) = -1, \quad \left(\frac{q}{p}\right) = -1,$$

et réciproquement.

3e *Cas.* — On donne les deux nombres premiers q et q_1.

Supposons $\left(\frac{q}{q_1}\right) = -1$, on sait que $\left(\frac{-1}{q_1}\right) = -1$, et par suite

$$\left(\frac{-q}{q_1}\right) = +1.$$

Le nombre q_1 se décompose dans le corps imaginaire $k(\sqrt{-q})$, et, comme $-q \equiv 1$ (4), et que le discriminant du corps a un nombre impair de classes, il en résulte, comme précédemment, que

$$\left(\frac{q}{q_1}\right) = +1.$$

Si $\left(\frac{q}{q_1}\right) = +1$, le raisonnement précédent ne donne plus $\frac{q_1}{q}$. D'après M. Hilbert, nous considèrerons le corps $k(\sqrt{qq_1})$. Pour ce corps, $m = q \cdot q_1 \equiv 1$ (4) et $d = qq_1$. Les seuls nombres premiers divisibles par des carrés d'un idéal premier sont q et q_1. Posons

$(q) = \mathfrak{q}^2$, $(q_1) = \mathfrak{q}_1^2$, $\mathfrak{q}$, $\mathfrak{q}_1$, $\mathfrak{q}\mathfrak{q}_1$ seront les seuls idéaux ambiges du corps. $\mathfrak{q}\mathfrak{q}_1$ est un idéal principal, et l'on peut démontrer que $\mathfrak{q}$ et $\mathfrak{q}_1$ sont aussi des idéaux principaux. On en conclut la valeur de $\left(\frac{q_1}{q}\right)$.

Soit ε l'unité fondamentale de $k(\sqrt{qq_1})$, on a $n(\varepsilon) = +1$, car $\left(\frac{-1}{q}\right) = -1$, $\left(\frac{-1}{q_1}\right) = -1$. On pourra donc trouver un nombre entier du corps α, tel que $\varepsilon = \frac{\alpha}{\alpha'}$ ou $(\alpha) = (\alpha')$. L'idéal α est donc tel que chacun de ses facteurs divise (α'). Soit maintenant η, une unité du corps telle que $\alpha = \eta \,.\, a$ ou $\alpha = \eta\sqrt{qq_1}$, on aurait

$$\varepsilon = \frac{\alpha}{\alpha'} = \frac{\eta a}{\eta' a} = \pm \eta^2 \quad \text{ou} \quad \varepsilon = \frac{\eta\sqrt{qq}}{-\eta'\sqrt{qq_1}} = \pm \eta^2.$$

ce qui est contraire à l'hypothèse que ε est une unité fondamentale. α ne pouvant être divisible, à la fois, par $\mathfrak{q}$ et $\mathfrak{q}'$, on ne peut avoir que

$$(\alpha) = (a)\mathfrak{q}, \qquad (\alpha) = (a)\mathfrak{q}_1.$$

dans les deux cas

$$\mathfrak{q} \sim 1, \qquad \mathfrak{q}_1 \sim 1.$$

Donc, pour les normes

$$\pm q_1 = \left(x + \frac{y}{2}\right)^2 - \frac{qq_1}{4} y^2$$
$$\pm 4q_1 = (2x + y)^2 - qq_1 y^2.$$

Ceci n'est possible que si $2x + y$ est divisible par q_1, et on peut écrire alors

$$\pm 4 = q_1 X^2 - qY^2$$

L'hypothèse $\left(\frac{q}{q_1}\right) = 1$ va nous permettre de déterminer le signe du premier membre, car on peut écrire

$$qY^2 \pm 4 \equiv 0 \ (q_1)$$
$$Y_1^2 \pm 4q \equiv 0 \ (q_1).$$

l'hypothèse exige que nous prenions le signe —, on a donc

$$-4 = q_1 X^2 - qY^2.$$

c'est-à-dire

$$q_1 X^2 = -4 (q), \quad X_1^2 = -4 q_1 (q),$$

c'est-à-dire que $\left(\frac{q}{q_1}\right) = +1$ entraîne $\left(\frac{-q_1}{q}\right) = +1$, et par suite $\left(\frac{q_1}{q}\right) = -1$, parce que $\left(\frac{-1}{q}\right) = -1$.

On a donc, pour

$$\left(\frac{q}{q_1}\right) = +1, \quad \left(\frac{q_1}{q}\right) = -1,$$

et aussi pour

$$\left(\frac{q}{q_1}\right) = -1, \quad \left(\frac{q_1}{q}\right) = +1,$$

ce qui démontre la loi de réciprocité pour les nombres premiers q et q_1. On a donc, en somme, le *théorème :*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}},$$

p et q représentant deux nombres premiers impairs quelconques, ce théorème est complété par les deux théorèmes suivants :

1er *Théorème complémentaire* :

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}.$$

2e *Théorème complémentaire* :

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Fermat connaissait déjà ces deux théorèmes. Le premier a été démontré, pour la première fois, par Euler, en 1783, le second, par Lagrange, en 1775. Gauss a découvert le premier théorème complémentaire en 1795.

Nous allons appliquer cette loi de réciprocité.

Nous allons pouvoir facilement déterminer la valeur de $\left(\frac{m}{p}\right)$, m étant quelconque, et p un nombre premier.

1. $\left(\frac{6}{7}\right)$, on a $\left(\frac{a \cdot b}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$,

$$\left(\frac{6}{7}\right) = \left(\frac{2}{7}\right)\left(\frac{3}{7}\right) = \left(\frac{3}{7}\right).$$

$$\left(\frac{3}{7}\right)\left(\frac{7}{3}\right) = -1. \quad \left(\frac{3}{7}\right) = -\left(\frac{7}{3}\right).$$

$7 \equiv 1\ (3)$, donc $\left(\frac{7}{3}\right) = \left(\frac{1}{3}\right) = +1$, donc enfin $\left(\frac{3}{7}\right) = -1$, et par suite $\left(\frac{6}{7}\right) = -1$.

2. $\left(\frac{27}{17}\right)$,

$$\left(\frac{27}{17}\right) = \left(\frac{10}{17}\right) = \left(\frac{2}{17}\right)\left(\frac{5}{17}\right) = \left(\frac{5}{17}\right).$$

$$\left(\frac{5}{17}\right) = \left(\frac{17}{5}\right) = \left(\frac{2}{5}\right) = -1.$$

$$\left(\frac{27}{17}\right) = -1.$$

On aurait pu dire $\left(\frac{27}{17}\right) = \left(\frac{3}{17}\right)^3$ et ainsi de suite, ou

$$\left(\frac{27}{17}\right) = \left(\frac{-7}{17}\right) = \left(\frac{7}{17}\right) = \left(\frac{17}{7}\right) = \left(\frac{3}{7}\right) = -1.$$

Jacobi a généralisé le théorème de réciprocité sous sa forme symbolique, cette généralisation nous sera utile plus loin.

Soit p, q, r ... des nombres premiers impairs, a un nombre premier avec chacun d'eux, posons par définition

$$\left(\frac{a}{p \cdot q \cdot r \ldots}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{q}\right)\left(\frac{a}{r}\right) \cdots$$

on a, pour tout entier impair P

$$\left(\frac{-1}{P}\right) = (-1)^{\frac{P-1}{2}}.$$

$$\left(\frac{2}{P}\right) = (-1)^{\frac{P^2-1}{8}}.$$

De plus, si P et Q sont deux nombres premiers impairs,

$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = (-1)^{\frac{P-1}{2} \times \frac{Q-1}{2}}.$$

La démonstration, que nous ne donnerons pas ici s'obtient par la méthode d'induction. On y parvient aussi en partant de

$$P = [(p - 1) + 1][(p_1 - 1) + 1] \ldots [(p_\nu - 1) + 1],$$

c'est-à-dire

$$P - 1 = 4a + (p - 1) + (p_1 - 1) + \ldots (p_\nu - 1),$$

où a est un nombre entier rationnel.

Il faut encore ici traiter à part le cas général et les cas complémentaires.

26. La représentations des nombres par des sommes de carrés. — Nous allons déduire, de la théorie des idéaux, quelques théorèmes bien connus.

I. — On a montré, au n° 4, que dans le corps $k(\sqrt{-1})$, tout nombre premier p, de la forme $4n + 1$, et le nombre $p = 2$, n'est susceptible que d'une décomposition essentielle de la forme

$$(1) \qquad p = (x + \sqrt{-1}\,y)(x - \sqrt{-1}\,y),$$

les facteurs de toute autre décomposition ne pouvant différer de ceux-ci que par des racines de l'unité ± 1, $\pm\sqrt{-1}$. Autrement dit : tout nombre premier $p \equiv 1 \ (4)$ ou $p = 2$ ne peut être mis que d'une façon sous la forme

$$(2) \qquad p = x^2 + y^2.$$

Legendre avait déjà montré comment on peut trouver x et y, dans le développement de $\sqrt{p}$, en fraction continue. Dans bien des cas, on obtient tout aussi vite x et y par des essais. Ce qui suit permet d'abréger ces essais.

De $p = x^2 + y^2$, on déduit

$$(zx)^2 + 1 \equiv 0 \ (p),$$

y étant premier avec p. Soit w une racine de la congruence

$$X^2 + 1 \equiv 0 \ (p).$$

x est un diviseur d'un des entiers $w + ap$, qui est $< p$, et que l'on

peut supposer $< \sqrt{\frac{p}{2}}$, il suffira donc de prendre pour a des nombres tels que $x + ap$ soit compris entre

$$-\frac{p}{2}\sqrt{\frac{p}{2}}, \qquad +\frac{p}{2}\sqrt{\frac{p}{2}}.$$

Soient p, p_1 deux nombres premiers de la forme $4n+1$, on a dans $k(\sqrt{-1})$

$$p = (x + \sqrt{-1}\,y)(x - \sqrt{-1}\,y)$$
$$p_1 = (x_1 + \sqrt{-1}\,y_1)(x_1 - \sqrt{-1}\,y_1),$$

on a donc

$$\begin{aligned} pp_1 &= (x + \sqrt{-1}\,y)(x_1 + \sqrt{-1}\,y_1)(x - \sqrt{-1}\,y)(x_1 - \sqrt{-1}\,y_1) \\ &= [xx_1 - yy_1 + (x_1y + xy_1)\sqrt{-1}][xx_1 - yy_1 - (x_1y + xy_1)\sqrt{-1}], \end{aligned}$$

(3) $\quad pp_1 = (X + \sqrt{-1}\,Y)(X - \sqrt{-1}\,Y) = X^2 + Y^2.$

ou

$$\begin{aligned} pp_1 &= (x + \sqrt{-1}\,y)(x_1 - \sqrt{-1}\,y_1)(x - \sqrt{-1}\,y)(x_1 + \sqrt{-1}\,y_1) \\ &= [xx_1 + yy_1 + (x_1y - xy_1)\sqrt{-1}][xx_1 + yy_1 - (x_1y - xy_1)\sqrt{-1}], \end{aligned}$$

(4) $\quad pp_1 = (X_1 + \sqrt{-1}\,Y_1)(X_1 - \sqrt{-1}\,Y_1) = X_1^2 + Y_1^2.$

pp_1 nous apparaît comme la norme de deux entiers du corps, pp_1 peut être mis, de deux façons essentielles, sous forme d'une somme de deux carrés, les formes (3) et (4).

Pour $p_1 = 2$, on a

$$2p = (1 + \sqrt{-1})(1 - \sqrt{-1})(x + \sqrt{-1}\,y)(x - \sqrt{-1}\,y),$$

mais comme $1 + \sqrt{-1} = \sqrt{-1}(1 - \sqrt{-1})$, $2p$ ne peut être mis que d'une seule manière, sous forme d'une somme de deux carrés.

On peut étendre ces considérations à un nombre quelconque, et on obtient (comme le lecteur pourra s'en convaincre lui-même) le théorème suivant, établi par Gauss [1].

---

[1] *Disquis. arith.*, V, 182.

Théorème. — Tout entier rationnel positif

$$a = 2^{\lambda} . Q . p_1^{e_1} p_2^{e_2} \dots p_\nu^{e_\nu},$$

qui contient les facteurs $p_1 \dots p_\nu$ de la forme $4n + 1$, avec des exposants entiers quelconques, et où Q est un produit de nombres de la forme $4n + 3$, avec des exposants pairs, peut être mis de plusieurs façons, sous la forme de deux carrés

$$a = x^2 + y^2.$$

Si l'un des facteurs $e_1, e_2, \dots, e_\nu$ est impair, on a

$$E = \frac{1}{2}(e_1 + 1)(e_2 + 1) \dots (e_\nu + 1),$$

décompositions distinctes, et si tous les exposants sont pairs, il y en a $E - \frac{1}{2}$.

Dans le cas où Q contient un facteur premier de la forme $4n + 3$ à une puissance impaire, a ne peut jamais être mis sous la forme

$$a = x^2 + y^2.$$

La réciproque de ce théorème permet de reconnaître si un nombre de la forme $4n + 1$ est premier.

Remarque : Gauss [1] a donné une solution intéressante et simple de l'équation

$$p = x^2 + y^2,$$

pour p premier.

Soit $p = 4n + 1$, x le nombre impair, y le nombre pair de la décomposition, et si de plus

$$q = 1 . 2 \dots n,$$
$$r = (n + 1)(n + 2) \dots 2n,$$

$\pm x$ est le plus petit reste obtenu en divisant $\frac{r}{2q}$ par p ; et y, le plus petit reste obtenu en divisant $\frac{1}{2} r^2$ par p.

---

(1) *Œuvres*, t. II, p. 89-91.

II. — Le corps $k(\sqrt{-2})$ n'a d'autres unités que ± 1, et le nombre des classes $h = 1$. Le nombre premier $p = 2 = -(\sqrt{-2})^2$, et tout nombre premier de la forme $8n + 1$ ou $8n + 3$ ne peut être décomposé, que d'une manière essentielle, en un produit de deux nombres premiers distincts

$$p = (x - \sqrt{-2}\,y)(x + \sqrt{-2}\,y).$$

Autrement dit :

Tout nombre premier positif p, de la forme $8n + 1$ ou $8n + 3$, ne peut être mis que d'une manière, sous la forme

$$p = x^2 + 2y^2,$$

x et y étant des entiers rationnels.

III. — Dans le corps $k(\sqrt{-3})$ $h = 1$, et tout nombre p est décomposable d'une seule manière essentielle, lorsque $\left(\frac{-3}{p}\right) = +1$, ce qui n'arrive que pour les nombres premiers de la forme $3n + 1$.

Soit p un pareil nombre,

$$p = \left(x + y\,\frac{1 + \sqrt{-3}}{2}\right)\left(x + y\,\frac{1 + \sqrt{-3}}{2}\right)$$

admet toujours une solution unique, telle que x soit impair et y soit pair. Soit

$$p = (a + b\omega)(a + b\omega').$$

a et b ne peuvent être tous deux pairs, sans quoi le second membre serait divisible par 4. Les unités du corps sont ± 1, ω, ω' dans le cas où a est impair et b pair, la condition est remplie par

$$(1) \qquad a + b\omega.$$

dans le cas où a est pair et b impair, la condition est remplie par

$$(2) \qquad (a + b\omega)\,\omega'.$$

Enfin si a et b sont impairs, elle est remplie par

$$(a + b\omega)\,\omega = -b\omega + (a + b)\,\omega.$$

c'est-à-dire que pour $p \equiv 1\ (3)$, il n'y a qu'une décomposition de la forme

$$p = (x_1 + y_1\sqrt{3})(x_1 - y_1\sqrt{3}),$$

ou encore, tout nombre premier rationel p, de la forme $3n + 1$, ne peut être mis, que d'une manière, sous la forme

$$p = x^2 + 3y^2.$$

On pourrait étendre ces théorèmes, à la représentation de nombres non premiers, par les formes $x^2 + 2y^2$, $x^2 + 3y^2$, et on pourrait aussi déduire, de la théorie des idéaux, d'autres représentations particulières de nombres, par des formes $x^2 \pm my^2$, nous y reviendrons plus tard, aux n[os] 35, 36, 37. Nous nous contenterons de ces exemples. Mais nous allons tirer quelques conséquences de la théorie des formes réelles.

Considérons le corps $k(\sqrt{2})$, pour lequel $h = 1$.

Dans ce corps, les nombres premiers p, de la forme $8n \pm 1$, se décomposent. Mais, comme ce corps contient une infinité d'unités qui s'obtiennent en formant les puissances de l'unité fondamentale $1 + \sqrt{2}$, la décomposition unique en idéaux premiers

$$(p) = (x + y\sqrt{2})(x - y\sqrt{2})$$

nous donne une infinité de représentations de $\pm p$, sous la forme $x^2 - 2y^2$, car si

$$p = x^2 - 2y^2,$$

on a

$$-p = (x + 2y)^2 - 2(x - y)^2,$$

ou

$$-p = (x - 2y)^2 - 2(x - y)^2,$$

car

$$-p = (x + y\sqrt{2})\varepsilon . (x - y\sqrt{2})\varepsilon',$$

de même

$$p = (x + y\sqrt{2})\varepsilon^2 . (x - y\sqrt{2})\varepsilon'^2,$$
$$p = (3x + 4y)^2 - 2(2x + 3y)^2.$$

On a donc le théorème :

Tout nombre premier positif ou négatif, qui pris positivement est de la forme $8n \pm 1$, peut être mis d'une infinité de façon sous la forme

$$x^2 - 2y^2,$$

et ces différentes formes se déduisent de l'une d'entre elles, en employant les unités $\pm \varepsilon^a$ du corps.

On peut énoncer quantités de théorèmes analogues.

27. Le symbole d'Hilbert pour les restes normiques. — Nous allons entreprendre une recherche assez longue, celle de la répartition des classes d'idéaux en genres.

Il s'agit d'une classification empruntée à la théorie des formes quadratiques, telle qu'elle a été établie, pour la première fois, par Gauss. Il lui a consacré la plus grande partie de la sect. V des *Disquis. arith.* Il considérait ces recherches sur les genres comme des plus belles et des plus difficiles de l'arithmétique supérieure.

Nous déduirons, de cette répartition de classes en genres, une nouvelle démonstration du théorème de réciprocité quadratique. Cette démonstration présente, sur toutes les autres, un grand avantage, elle peut être généralisée pour les lois de réciprocité de degré supérieur.

M. Hilbert a beaucoup simplifié l'exposition pour le corps quadratique, il lui a donné une forme qui restera longtemps classique, et cela au moyen d'un nouveau symbole, que nous allons définir tout d'abord.

Définition : Soit p un nombre premier positif rationnel, et soient m et n deux nombres entiers rationnels quelconques, m ne contenant aucun facteur carré.

Si, pour toute puissance entière positive de p, p^e, n est congru à la norme d'un entier α du corps $k(\sqrt{m})$, suivant le module p^e, c'est-à-dire si $n \equiv n(\alpha((p^e)$ pour toute valeur rationnelle entière positive e. Nous conviendrons que

$$\left(\frac{n,\, m}{p}\right) = +1.$$

Si, par contre, il n'y a dans le corps $k(\sqrt{m})$ aucun nombre α, tel que $n \equiv n(\alpha)\ (p)$, ou si la congruence $n \equiv n(\alpha)\ (p^e)$ n'est pas

satisfaite pour toutes les valeurs entières et rationnelles de e par des entiers α du corps, nous écrirons

$$\left(\frac{n,\ m}{p}\right) = -1.$$

Dans le premier cas, n est dit un *reste normique* du corps $k(\sqrt{m})$ suivant le module p; dans le second cas, il est dit un *non-reste normique* suivant le module p.

La raison essentielle de l'emploi de ce symbole, c'est qu'il peut être soumis à des règles de calcul très simples, analogues aux règles valables pour le symbole de Legendre.

Avant de les expliquer, nous ferons les remarques suivantes :

1. On peut toujours supposer que n est un entier sans facteur carré, car si $n = a^2 n_1$, on a

$$\left(\frac{n,\ m}{p}\right) = \left(\frac{n_1,\ m}{p}\right).$$

2. Parmi les $p - 1$, nombres incongrus du système

$$1,\ 2\ \ldots\ p - 1,$$

la moitié est formée de restes quadratiques, l'autre moitié est formée de non-restes suivant p. Désignons par

$$r_1,\ r_2,\ \ldots\ r_{\frac{p-1}{2}},$$

les restes, et par

$$n_1,\ n_2,\ \ldots\ n_{\frac{p-1}{2}}$$

les non-restes quadratiques.

Soit n un non-reste quelconque, parmi les différences

$$d_1 = r_1 - n, \quad d_2 = r_2 - n\ \ldots\ d_{\frac{p-1}{2}} = r_{\frac{p-1}{2}} - n,$$

il y a, au moins, un non-reste suivant p.

La proposition est évidente pour $p = 3$.

Soit p un nombre premier > 3, on voit tout d'abord que deux quelconques des différences d, ne peuvent être congrues suivant p. Il en résulte, que deux des nombres d, ne peuvent être congrus au même reste.

Admettons que tous les nombres d_1, d_2 ... soient des restes, on aurait

$$d_1 \equiv r_{k_1} \ (p),$$

ou

$$r_1 - n \equiv r_{k_1} \ (p)$$
$$n \equiv r_1 - r_{k_1} \ (p)$$

et de même

$$n \equiv r_2 - r_{k_2} \ (p)$$
$$\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot$$
$$n \equiv r_{p-1} - r_{k_{p-1}} \ (p),$$

où les r_{k_1}, ... $r_{k_{p-1}}$ coïncident avec les r_1, r_2 ... r_{p-1} pris dans un certain ordre. En ajoutant toutes ces congruences, il vient

$$\frac{p-1}{2} \cdot n \equiv 0 \ (p),$$

ce qui est impossible, car $\frac{p-1}{2}$ et n sont premiers avec p. Il y a donc, parmi les différence d, au moins un non-reste.

Si l'on remarque de plus, que pour $p > 3$ (le cas de $p = 3$ doit être excepté),

$$\sum_{1}^{\frac{p-1}{1}} r_i \quad \text{et} \quad \sum_{2}^{\frac{p-1}{1}} n_i \quad \text{sont} \equiv 0 \ (p),$$

on voit que parmi les nombres d_i il y a au moins un reste.

Désignons par r l'un quelconque des nombres r_i, on démontre de la même façon que dans les suites

$$n_i - r, \qquad n_i \pm r, \qquad n_i \pm n,$$

il y a toujours des restes et des non-restes.

Les opérations, sur le symbole de Hilbert, sont fondées sur les propriétés exprimées par les 4 théorèmes suivants.

Théorème I. — p étant un nombre premier impair, qui ne divise aucun des deux entiers rationnels m et n, on a toujours

$$\text{(A)} \qquad \left(\frac{n,\ m}{p}\right) = +1.$$

$$\text{(B)} \qquad \left(\frac{n,\ p}{p}\right) = \left(\frac{p,\ n}{p}\right) = \left(\frac{n}{p}\right).$$

Si n et m sont tous deux divisibles par la première puissance de p, et ne le sont pas par p^2, on a

$$\text{(C)} \qquad \left(\frac{n,\ m}{p}\right) = \left(\frac{-\frac{nm}{p^2}}{p}\right).$$

Démonstration : A. Soit d'abord

$$m \not\equiv 1\ (4),$$

le théorème exige, tout d'abord, que la congruence

$$n \equiv x^2 - my^2\ (p),$$

ou

$$\text{(1)} \qquad x^2 - my^2 - n \equiv 0\ (p),$$

admette des solutions entières rationnelles.

En effet, si $\left(\frac{n}{p}\right) = +1$, $\left(\frac{m}{p}\right) = \pm 1$, on peut prendre pour y la valeur 0, et pour x, une solution de

$$x^2 - n \equiv 0\ (p).$$

Si $\left(\frac{m}{p}\right) = +1$, $\left(\frac{n}{p}\right) = \pm 1$, on peut écrire $m \equiv z^2\ (p)$, et la congruence (1) peut s'écrire

$$\text{(2)} \qquad x^2 - z^2y^2 - n \equiv 0\ (p),$$

on peut poser

$$\text{(3)} \qquad x \equiv \frac{n+1}{2}\ (p),$$

$$\text{(4)} \qquad zy \equiv \frac{n-1}{2}\ (p),$$

où l'on remplacera n par son reste, par p si n est pair.

Mais la congruence (4) admet toujours une solution entière pour y, parce que 2 est premier avec p, par conséquent (1) admet des solutions entières x et y.

Soit enfin $\left(\frac{n}{p}\right) = -1$, $\left(\frac{m}{p}\right) = -1$. On remarque que my^2 parcourt deux fois tous les non-restes de p, lorsqu'on donne à y les valeurs de 1, 2, ... $p-1$. Si, d'autre part, on donne à x^2 toutes les valeurs des restes suivant p, il y a parmi les nombres $x^2 - n$ au moins un non-reste, la congruence (1) admet donc au moins une solution entière x, y.

Pour $m \equiv 1 \ (4)$ il faut que l'on puisse résoudre

$$n \equiv \left(x + \frac{y}{2}\right)^2 - \frac{m}{4} y^2 \ (p),$$

ou

$$(1_a) \qquad 4n \equiv (2x + y)^2 - my^2 \ (p).$$

Des considérations analogues aux précédentes nous montreront que (1_a) est possible.

Après avoir prouvé qu'il y a toujours un nombre α du corps, tel que

$$n \equiv n(\alpha) \ (p),$$

il nous reste à prouver que, quel que soit e, il existe un nombre α, tel que

$$n \equiv n(\alpha) \ (p^e).$$

Nous le supposerons vrai pour $e - 1$, et nous le déduirons pour e.

Soit $\alpha_1 = a + b\omega$ un nombre entier du corps $k(\sqrt{m})$, tel que $n \equiv n(\alpha_1) \ (p^{e-1})$, posons $x = a + up^{e-1}$, $y = b + vp^{e-1}$, et cherchons à déterminer u et v, de telle sorte que

$$n \equiv n(x + y\omega) \ (p^e).$$

Lorsque $m \not\equiv 1 \ (4)$ par exemple, u et v devront satisfaire à

$$2au - 2bv - \frac{a^2 - b^2 m - n}{p^{e-1}} \equiv 0 \ (p).$$

Cette congruence admet toujours des solutions, car a et b ne peuvent tous deux être divisibles par p.

On verrait qu'il en est de même pour $m \equiv 1$ (4).

La congruence $n = n(x + y\omega)$ (p^e) admet une solution au moins pour $e = 1$, elle en admet donc pour $a = 2, 3, \ldots$, on a donc en général

$$\left(\frac{n, m}{p}\right) = 1.$$

B. Soit $m = p$ la condition nécessaire et suffisante pour que les congruences

$$(5) \qquad x^2 - py^2 - n \equiv 0 \ (p^e), \qquad p \not\equiv 1 \ (4),$$

$$(6) \qquad (2x + y)^2 - py^2 - 4n \equiv 0 \ (p^e), \qquad p \equiv 1 \ (4)$$

soient possibles est $\left(\frac{n}{p}\right) = 1$. Si enfin $n = p$, la congruence

$$x^2 - my^2 - p \equiv 0 \ (p^e),$$

n'est possible que si

$$x^2 - my^2 \equiv 0 \ (p)$$

est possible, c'est-à-dire si $\left(\frac{m}{p}\right) = +1$, par conséquent

$$\left(\frac{n, p}{p}\right) = \left(\frac{p, n}{p}\right) = \left(\frac{n}{p}\right).$$

Cette dernière égalité s'étend évidemment au cas où soit m soit n est divisible par p,

$$\left(\frac{pn_1, m}{p}\right) = \left(\frac{m, pn_1}{p}\right) = \left(\frac{m}{p}\right).$$

C. Si m et n sont tous deux divisibles par p, sans l'être tous deux par p^2, $(m = pm_1, \ n = pn_1)$, les congruences

$$x^2 - my^2 - n \equiv 0 \ (p^e),$$
$$(2x + y)^2 - my^2 - 4n \equiv 0 \ (p^e),$$

n'admettent de solutions que si l'on peut résoudre une congruence de la forme

$$pX^2 - m_1Y^2 - n_1 \equiv 0 \ (p),$$

pour cela, il faut et il suffit que

$$m_1 Y^2 + n_1 \equiv 0 \ (p),$$

ou encore que

$$(m_1 Y)^2 + m_1 n_1 \equiv 0 \ (p)$$

soit possible, c'est-à-dire que

$$\left(\frac{-m_1 n_1}{p}\right) = +1,$$

c'est-à-dire que

$$\left(\frac{n, m}{p}\right) = \left(\frac{-\frac{n.m}{p^2}}{p}\right).$$

Le théorème I est donc complètement démontré.

Théorème II. — Lorsque m et n sont deux entiers rationnels impairs, on a

$$\text{(A)} \qquad \left(\frac{n, m}{2}\right) = (-1)^{\frac{n-1}{2}\cdot\frac{m-1}{2}},$$

et

$$\text{(B)} \qquad \left(\frac{n, 2}{2}\right) = \left(\frac{2, n}{2}\right) = (-1)^{\frac{n^2-1}{8}}.$$

Démonstration : Démontrer A, cela revient à démontrer que

$$(1) \qquad x^2 - my^2 - n \equiv 0 \ (2^\nu)$$

admet des solutions pour $m \not\equiv 1$ (4), et que

$$(2) \qquad x^2 + xy + \frac{1-m}{4} y^2 - n \equiv 0 \ (2^\nu)$$

en admet pour $m \equiv 1$ (4).

Démontrer B, c'est démontrer que

$$(3) \qquad x^2 - 2y^2 - n \equiv 0 \ (2^\nu)$$

$$(4) \qquad x^2 - ny^2 - 2 \equiv 0 \ (2^\nu)$$

ou que

$$(5) \qquad x^2 + xy + \frac{1-n}{4} y^2 - 2 \equiv 0 \ (2^\nu).$$

suivant que $n \not\equiv 1$ ou que $n \equiv 1$ (4) admettent des solutions.

On reconnaît tout d'abord que ces congruences sont possibles pour $e = 1$, mais que cela n'entraîne pas la possibilité des congruences pour $e > 2$. Nous allons montrer que ces congruences sont possibles pour toutes les valeurs de e, si elles sont possibles pour $e = 3$.

Soit $x = a$, $y = b$, une solution de la congruence

(1), (3), (4) $$x^2 - my^2 - n \equiv 0 \; (2^3)$$

[en réunissant les congruences analogues (1), (3), (4)], supposons en outre que

$$a^2 - mb^2 - n$$

n'est pas divisible par 2^4, et posons

$$x = a + 2^2u, \quad y = b + 2^2v,$$

alors

$$x^2 - my^2 - n = a^2 - mb^2 - n + 8(au - mbv) + 16(u^2 - mv^2),$$

c'est-à-dire que

$$x^2 - my^2 - n \equiv 0 \; (2^4),$$

si

$$\frac{a^2 - mb^2 - n}{8} + au - mbv \equiv 0 \; (2),$$

c'est-à-dire

(6) $$au - mbv + 1 \equiv 0 \; (2).$$

Mais la congruence (1) exige que a ou b soit impair, et les congruences (3) et (4) exigent que a soit impair, la congruence (6) est donc possible.

On concluera de même de la possibilité de $x^2 - my^2 - n \equiv 0 \; (2^e)$ pour $e = 4$, celle de la même congruence pour $e = 5, 6, \ldots$.

Il est facile de voir que pour appliquer ce raisonnement à la congruence 3, où $m = 2$, il faut légèrement modifier les valeurs de x et y.

On montre de la même manière, que les congruences (2) et (5) admettent des solutions pour toutes les valeurs de $e > 3$, lorsqu'elles en admettent pour $e = 3$. Soit $x = u$, $y = b$ une solution de ces

congruences pour $e = 3$, on posera $x = a + 8u$, $y = b + 8v$, il faut alors déterminer u, v de telle sorte que l'on ait

$$x^2 + xy + \frac{1-m}{4} y^2 - n \equiv 0 \pmod{2^4},$$

$$x^2 + xy + \frac{1-n}{4} y^2 - 2 \equiv 0 \pmod{2^4}.$$

On serait conduit à résoudre

$$av + bu + 1 \equiv 0 \pmod{2},$$

qui admet toujours des solutions, car la congruence (2) exige que a ou b soit impair, et la congruence (5) exige que b soit impair.

Pour reconnaître enfin, pour quelles valeurs de m et de n, les congruences de (1) à (5) admettent des solutions quel que soit e, il suffit d'essayer pour m et n toutes les combinaisons 1, 2, 3, 5, 7, dans les congruences

$$x^2 - my^2 - n \equiv 0 \pmod{8},$$

$$x^2 + xy + \frac{1-m}{4} y^2 - n \equiv 0 \pmod{8}.$$

Toutefois, pour déduire un résultat qui nous sera utile dans la démonstration du théorème suivant, nous donnerons aussi à m et n les valeurs 6. On obtient alors le tableau suivant :

m	n
1	1, 2, 3, 5, 6, 7
2	1, 2, 7
3	1, 5, 6
5	1, 3, 5, 7
6	1, 3, 6
7	1, 2, 5

où nous avons écrit, en face des valeurs de m, les valeurs de n correspondantes rendant les congruences possibles.

Ce tableau nous montre que si m et n sont impairs,

(A) $$\left(\frac{n, m}{2}\right) = (-1)^{\frac{n-1}{2}\cdot\frac{m-1}{2}};$$

de plus, si n est impair,

$$\left(\frac{2, n}{2}\right) = \left(\frac{n, 2}{2}\right) = +1 \quad \text{ou} \quad -1,$$

suivant que $n \equiv \pm 1\ (8)$ ou $n \equiv \pm 3\ (8)$, ce qui nous donne

(B) $$\left(\frac{2, n}{2}\right) = \left(\frac{2, n}{2}\right) = (-1)^{\frac{n^2-1}{8}}.$$

Le tableau peut aussi nous servir pour le cas de $p = 2$, m ou n étant pair, ou m et n étant pairs tous deux.

Théorème III. — Si m, n, m_1, n_1 sont des entiers rationnels impairs, on a

(A) $$\left(\frac{n, 2m_1}{2}\right) = \left(\frac{n, 2}{2}\right)\left(\frac{n, m_1}{2}\right).$$

(B) $$\left(\frac{2n_1, m}{2}\right) = \left(\frac{2, m}{2}\right)\left(\frac{n_1, m}{2}\right).$$

(C) $$\left(\frac{2n_1, 2m_1}{2}\right) = \left(\frac{-m_1n_1, 2m_1}{2}\right).$$

Démonstration : A. On reconnaît, comme précédemment, que la condition nécessaire et suffisante pour que

$$x^2 - 2m_1y^2 - n \equiv 0\ (2^e)$$

soit soluble, est qu'elle le soit pour $e = 3$. Il suffira donc de prendre, pour $2m_1$ et n, les nombres inscrits au tableau.

Ce qui permet de vérifier

$$\left(\frac{n, 2m_1}{2}\right) = (-1)^{\frac{n^2-1}{8} + \frac{n-1}{2}\cdot\frac{m_1-1}{2}},$$

c'est-à-dire

(A) $$\left(\frac{n, 2m_1}{2}\right) = \left(\frac{n, 2}{2}\right)\left(\frac{n, m_1}{2}\right).$$

B. Pour déterminer la valeur du symbole $\left(\frac{2n_1, m}{2}\right)$, nous considérons deux cas, $m \equiv 3\ (4)$, $m \equiv 1\ (4)$.

B_1. $m \equiv 3 \ (4)$. Le symbole d'Hilbert a la valeur $+1$, lorsque

$$x^2 - my^2 - 2n_1 \equiv 0 \ (2^e)$$

est possible pour toutes les valeurs de e. Ceci a encore lieu lorsque la congruence est possible pour $e = 3$, car dans ce cas les solutions sont des entiers impairs.

Mais le tableau nous montre que

$$\left(\frac{2n_1,\ m}{2}\right) = +1,$$

si $n \equiv 1 \ (4)$ et $m \equiv \pm 1 \ (8)$, ou si $n_1 \equiv 3 \ (4)$ avec $m \equiv 1 \ (8)$ ou $m \equiv 3 \ (8)$, ces formules réunis aux cas pour lesquels $\left(\frac{2n_1,\ m}{2}\right) = -1$, nous donnent

$$\left(\frac{2n_1,\ m}{2}\right) = (-1)^{\frac{m^2-1}{8} + \frac{n_1-1}{2} \cdot \frac{m-1}{2}},$$

c'est-à-dire

$$\left(\frac{2n_1,\ m}{2}\right) = \left(\frac{2,\ m}{2}\right)\left(\frac{n_1,\ m}{2}\right).$$

B_2. $m \equiv 1 \ (4)$. Dans cette hypothèse, il s'agit de savoir si la congruence

$$(1) \qquad x^2 + xy + \frac{1-m}{4} y^2 - 2n_1 \equiv 0 \ (2^e),$$

ou si la congruence

$$(1_a) \qquad (2x + y)^2 - my^2 - 8n_1 \equiv 0 \ (2^{e+2})$$

admet des solutions ; on peut l'écrire

$$(2) \qquad X^2 - mY^2 - 8n_1 \equiv 0 \ (2^{e_1}),$$

elle en admet toujours pour $e_1 = 2$, elle en admet pour $e_1 = 3$, si l'on peut satisfaire à (2_a). $X^2 - mY^2 \equiv 0 \ (8)$. Réciproquement, la congruence (2) n'est soluble pour $e_1 = 4$ et $e_1 > 4$, que si X et Y satisfont à $X^2 - mY^2 \equiv 0 \ (8)$ et non à $X^2 - mY^2 \equiv 0 \ (16)$, c'est-à-dire que X et Y ne doivent pas être des nombres pairs, et il en résulte que (2_a) n'admet de solutions que si $m \equiv 1 \ (8)$. Il y a alors des nombres x et y, solutions de la congruence primitive (1). Il s'ensuit, comme dans les cas précédents, que la congruence (2)

est possible pour toutes les valeurs de e_1, ou encore que (1) est soluble pour toutes les valeurs de e, dès que $m \equiv 1\ (8)$, la forme de n_1 n'intervient pas, on a

$$\left(\frac{2n_1,\ m}{2}\right) = +1 \quad \text{lorsque} \quad m \equiv 1\ (8),$$

$$\left(\frac{2n_1,\ m}{2}\right) = -1 \quad \text{lorsque} \quad m \equiv 5\ (8),$$

ou encore lorsque $m \equiv 1\ (4)$,

$$\left(\frac{2n_1,\ m}{2}\right) = (-1)^{\frac{n_1^2-1}{8}} = \left(\frac{2,\ m}{2}\right)\left(\frac{n_1,\ m}{2}\right).$$

En résumant les deux cas $m \equiv 1$, $m \equiv 3\ (4)$, on voit que

$$\text{(B)} \qquad \left(\frac{2n_1,\ m}{2}\right) = \left(\frac{2,\ m}{2}\right)\left(\frac{n_1,\ m}{2}\right).$$

C. La valeur du symbole $\left(\frac{2n_1,\ 2m_1}{2}\right)$ dépend des propriétés de la congruence

$$(1) \qquad x^2 - 2m_1y^2 - 2n_1 \equiv 0\ (2^e),$$

cette congruence admet des solutions, pour les valeurs de e, qui sont telles que

$$(1_a) \qquad 2m_1x^2 - (2m_1y)^2 - 4m_1n_1 \equiv 0\ (2^{e+1})$$

en admet. Ceci exige que x et $2m_1y$ soient pairs ; soit donc $x = 2X$, $m_1y = Y$, il vient

$$(1_b) \qquad Y^2 - 2m_1X^2 + m_1n_1 \equiv 0\ (2^{e-1}).$$

A chaque solution de (1) correspond une solution de (1_b) et réciproquement. C'est pourquoi

$$\left(\frac{2n_1,\ 2m_1}{2}\right) = \left(\frac{-m_1n_1,\ 2m_1}{2}\right).$$

Théorème IV. — Soient m, n, m_1, n_1 quatre entiers ration-

nels sans facteurs carrés, et soit p un nombre premier rationnel, on a

(A) $$\left(\frac{-m,\ m}{p}\right) = +1,$$

(B) $$\left(\frac{n,\ m}{p}\right) = \left(\frac{m,\ n}{p}\right),$$

(C) $$\left(\frac{nn_1,\ m}{p}\right) = \left(\frac{n,\ m}{p}\right)\left(\frac{n_1,\ m}{p}\right),$$

(D) $$\left(\frac{n,\ mm_1}{p}\right) = \left(\frac{n,\ m}{p}\right)\left(\frac{n,\ m_1}{p}\right).$$

Démonstration : L'égalité (A) est évidente, car $-m$ est la norme de $\sqrt{m}$, et on a pour tout nombre p, la congruence

$$-m \equiv n(\sqrt{m})\ (p).$$

B. La formule (B) est vraie pour p impair, car si n et m sont premiers avec p,

$$\left(\frac{n,\ m}{p}\right) = \left(\frac{m,\ n}{p}\right) = +1.$$

Si l'un des nombres m ou n est divisible par p,

$$\left(\frac{pm_1,\ m}{p}\right) = \left(\frac{m}{p}\right), \quad \left(\frac{m,\ pm_1}{p}\right) = \left(\frac{m}{p}\right),$$
$$\left(\frac{n,\ pm_1}{p}\right) = \left(\frac{n}{p}\right), \quad \left(\frac{pm_1,\ n}{p}\right) = \left(\frac{n}{p}\right).$$

Enfin si m et n sont divisibles par p^1,

$$\left(\frac{m,\ n}{p}\right) = \left(\frac{n,\ m}{p}\right) = \left(\frac{-\frac{mn}{p^2}}{p}\right).$$

En second lieu, la formule (B) est vraie pour $p = 2$. Le théorème III nous montre que le théorème est vrai pour les cas où l'un des nombres m ou n au moins est impair. Reste le cas de m et n pairs,

$$\left(\frac{n,\ m}{2}\right) = \left(\frac{2n_1,\ 2m_1}{2}\right) = \left(\frac{-m_1n_1,\ 2m_1}{2}\right) = \left(\frac{-m_1n_1,\ 2}{2}\right)\left(\frac{-m_1n_1,\ m_1}{2}\right)$$

et

$$\left(\frac{m,\ n}{2}\right) = \left(\frac{-m_1n_1,\ 2}{2}\right)\left(\frac{-m_1n_1,\ n_1}{2}\right).$$

Mais

$$\left(\frac{-m_1n_1,\ n_1}{2}\right) = (-1)^{\frac{-m_1n_1-1}{2}\cdot\frac{n_1-1}{2}},$$

$$\left(\frac{-m_1n_1,\ m_1}{2}\right) = (-1)^{\frac{-m_1n_1-1}{2}\cdot\frac{m_1-1}{2}},$$

et comme il résulte de $m_1 \equiv \pm 1$, $n_1 \equiv \pm 1$ (4),

$$\frac{-m_1n_1-1}{2} \times \frac{m_1-n_1}{2} \equiv 0\ (2),$$

c'est-à-dire que (B) est vraie pour $p = 2$.

C. La formule (C) est vraie, tout d'abord, pour p impair, dans le cas où nn_1 est premier avec p.

On a, ou bien

$$\left(\frac{nn_1,\ m}{p}\right) = 1 = \left(\frac{n,\ m}{p}\right)\left(\frac{n_1,\ m}{p}\right),$$

dans le cas où m n'est pas divisible par p, ou bien

$$\left(\frac{nn_1,\ pm_1}{p}\right) = \left(\frac{nn_1}{p}\right) = \left(\frac{n}{p}\right)\left(\frac{n_1}{p}\right) = \left(\frac{n,\ pm_1}{p}\right)\left(\frac{n_1,\ pm_1}{p}\right),$$

lorsque $p = pm_1$. On le démontre de même, lorsque nn_1 est divisible par p.

Pour $p = 2$, la formule (C) est une conséquence du troisième théorème, et de ce fait que si m, n, n_1 sont impairs,

$$\left(\frac{nn_1,\ m}{2}\right) = \left(\frac{n,\ m}{2}\right)\left(\frac{n_1,\ m}{2}\right),$$

et

$$\left(\frac{nn_1,\ 2}{2}\right) = \left(\frac{n,\ 2}{2}\right)\left(\frac{n_1,\ 2}{2}\right),$$

comme nous le démontrons facilement,

$$\left(\frac{n,\ m}{2}\right)\left(\frac{n_1,\ m}{2}\right) = (-1)^{\frac{m-1}{2}\left(\frac{n-1}{2}+\frac{n_1-1}{2}\right)},$$

car, à cause de l'hypothèse

$$\frac{n-1}{2}\cdot\frac{n_1-1}{2} \equiv 0 \ (2),$$

on a

$$\frac{n-1}{2} + \frac{n_1-1}{2} \equiv \frac{nn_1-1}{2} \ (2).$$

et par suite

$$\left(\frac{n,\ m}{2}\right)\left(\frac{n_1,\ m}{2}\right) = \left(\frac{nn_1,\ m}{2}\right).$$

L'égalité

$$\left(\frac{nn_1,\ 2}{2}\right) = \left(\frac{n,\ 2}{2}\right)\left(\frac{n_1,\ 2}{2}\right)$$

s'obtient par un calcul direct, en remarquant que

$$\frac{n^2n_1^2-1}{8} \equiv \frac{n^2-1}{8} + \frac{n_1^2-1}{8} \ (2).$$

D. La formule (D) se démontre en partant du symbole $\left(\frac{n,\ mm_1}{p}\right)$ et en lui appliquant la formule (B), puis la formule (C), puis enfin en appliquant à chaque facteur la formule (B).

Si alors on remarque que $\left(\frac{n,\ m}{p}\right) = +1$ pour tout nombre premier p, n étant la norme d'un entier α du corps $k(\sqrt{m})$, le théorème IV nous donne

$$\left(\frac{n\,.\,n(\alpha),\ m}{p}\right) = \left(\frac{n,\ m}{p}\right).$$

28. Le système des caractères d'un idéal. — Soit a un entier rationnel et soient $l_1, l_2 \ldots l_t$ les différents nombres premiers rationnels qui divisent le discriminant d du corps $k(\sqrt{m})$, d'après Gauss l'ensemble des t unités ± 1

$$\left(\frac{a,\ m}{l_1}\right)\left(\frac{a,\ m}{l_2}\right)\cdots\left(\frac{a,\ m}{l_t}\right)$$

est dit le *système des caractères du nombre a dans le corps* $k(\sqrt{m})$.

Pour étendre cette définition aux idéaux d'un corps, il faut faire une distinction entre les corps réels et les corps imaginaires.

Soit [1] $\mathfrak{a}$ un idéal d'un corps imaginaire $k(\sqrt{m})$, on peut toujours admettre que $\overline{n} = n(\mathfrak{a})$ est un nombre positif, et nous désignerons par *système des caractères de l'idéal* $\mathfrak{a}$ *du corps* $k(\sqrt{m})$ l'ensemble des $r = t$ unités ± 1.

$$\left(\frac{\overline{n}, m}{l_1}\right)\left(\frac{\overline{n}, m}{l_2}\right)\cdots\left(\frac{\overline{n}, m}{l_t}\right).$$

Soit $\mathfrak{a}$ un idéal d'un corps réel $k(\sqrt{m})$, on établit d'abord le système des caractères E du nombre -1, et l'on distingue deux cas :

1. Le système des caractères n'est composé que d'unités positives.

2. Le système des caractères contient des unités positives et des unités négatives.

Dans le premier cas $\overline{n} = n(\alpha)$ est positif, et l'ensemble des $r (= t)$ unités qui forment l'ensemble des caractères de $\overline{n}$ est dit aussi l'ensemble des caractères de $\mathfrak{a}$.

Dans le second cas, soit l_t un nombre premier tel que

$$\left(\frac{-1, m}{l_t}\right) = -1,$$

nous choisirons $\overline{n} = \pm n(\mathfrak{a})$, nous prendrons le signe $+$ ou le signe $-$ de telle sorte que

$$\left(\frac{\overline{n}, m}{l_t}\right) = +1,$$

posons $r = t - 1$, et nous désignerons par système de caractères de $\mathfrak{a}$ dans le corps $k(\sqrt{m})$ les r unités

$$\left(\frac{\overline{n}, m}{l_1}\right)\left(\frac{\overline{n}, m}{l_2}\right)\cdots\left(\frac{\overline{n}, m}{l_r}\right).$$

Le système des caractères d'un idéal principal n'est donc composé que d'unités positives.

1er *Exemple.* — Le corps imaginaire $k(\sqrt{-21})$, $d = -84$.

---

(1) Hilbert, *Zahlber.*, § 65.

Nous avons à considérer les nombres premiers $l_1 = 2$, $l_2 = 3$, $l_3 = 7$, par exemple pour -1,

$$\left(\frac{-1, -21}{2}\right) = (-1)^{\frac{-1-1}{2}} = -1, \quad \left(\frac{-1, -21}{3}\right) = \left(\frac{-1}{3}\right) = -1,$$
$$\left(\frac{-1, -21}{7}\right) = +1,$$

pour le nombre 3,

$$\left(\frac{3, -21}{2}\right) = -1, \quad \left(\frac{3, -21}{3}\right) = \left(\frac{7}{3}\right) = +1, \quad \left(\frac{3, -21}{7}\right) = \left(\frac{3}{7}\right) = -1.$$

La norme de l'idéal ambigu $(2, 1 + \sqrt{-21})$, $\overline{n} = 2$, et on a

$$\left(\frac{2, -21}{2}\right) = -1, \quad \left(\frac{2, -21}{3}\right) = \left(\frac{2}{3}\right) = -1, \quad \left(\frac{2, -21}{7}\right) = +1.$$

Enfin soit $\mathfrak{a} = (5, 3 + \sqrt{-21})$, $\overline{n} = 5$,

$$\left(\frac{5, -21}{2}\right) = +1, \quad \left(\frac{5, -21}{3}\right) = \left(\frac{5}{3}\right) = -1, \quad \left(\frac{5, -21}{7}\right) = \left(\frac{5}{7}\right) = -1.$$

Pour tout idéal principal (α) le système des caractères est évidemment $+1$, $+1$, $+1$.

2e *Exemple.* — Le corps réel $k(\sqrt{34})$, $d = 136$, $l_1 = 2$, $l_2 = 17$.

$$\left(\frac{-1, 34}{2}\right) = (-1)^{\frac{1-1}{8} + \frac{1-1}{2} \cdot \frac{17-1}{2}} = +1,$$
$$\left(\frac{-1, 34}{17}\right) = \left(\frac{-1}{17}\right) = +1.$$

il faut donc faire $r = t = 2$.

Tout idéal principal admet comme caractère $+1$, $+1$.

Soit $\mathfrak{a} = (3, 1 + \sqrt{34})$, il faut prendre $\overline{n} = +3$, le système des caractères de $\mathfrak{a}$ est

$$\left(\frac{3, 34}{2}\right) = (-1)^{1+8} = -1, \quad \left(\frac{3, 34}{17}\right) = \left(\frac{3}{17}\right) = -1.$$

3e *Exemple.* — Le corps réel $k(\sqrt{51})$, $d = 204$, $l_1 = 2$, $l_3 = 3$, $l_2 = 17$, les caractères de -1 sont

$$\left(\frac{-1, 51}{2}\right) = -1, \quad \left(\frac{-1, 51}{3}\right) = \left(\frac{-1}{3}\right) = -1,$$
$$\left(\frac{-1, 51}{17}\right) = \left(\frac{-1}{17}\right) = 1.$$

Nous ferons $l_3 = 3$, $r = 2$, et nous aurons pour les caractères d'un idéal principal $+ 1$, $+ 1$.

Soit $\mathfrak{a} = (5, 6 + \sqrt{51})$,

$$\left(\frac{\bar{n}, 51}{3}\right) = \left(\frac{\bar{n}}{3}\right) = \left(\frac{\pm 5}{3}\right) = + 1,$$

si l'on prend $\bar{n} = - 5$, on a alors pour $\mathfrak{a}$

$$\left(\frac{-5, 51}{2}\right) = - 1, \quad \left(\frac{-5, 51}{17}\right)\left(\frac{5}{17}\right) = - 1.$$

On a comme conséquence immédiate de ce qui précède :

Théorème. — Tous les idéaux d'une même classe ont le même système de caractères.

Démonstration : Soient $\mathfrak{a}$ et $\mathfrak{b}$ deux idéaux du corps $k(\sqrt{m})$ appartenant à la même classe, c'est-à-dire qu'il existe deux entiers α et β du corps, tels que

$$(\alpha)\mathfrak{a} = (\beta)\mathfrak{b}.$$

Soient $n(\alpha)$ et $n(\beta)$ les normes de α et de β, et posons, suivant la définition des systèmes du caractère de $\mathfrak{a}$

$$N = \pm n(\alpha\mathfrak{a}), \quad N_1 = \pm n(\beta\mathfrak{b}),$$

c'est-à-dire

$$N = N_1,$$
$$\bar{n} = \pm n(\mathfrak{a}), \quad \bar{n}_1 = \pm n(\mathfrak{b}),$$

on a pour $p = l_1, l_2 \dots l_r$,

$$\left(\frac{N, m}{p}\right) = \left(\frac{n(\alpha), m}{p}\right)\left(\frac{\bar{n}, m}{p}\right) = \left(\frac{\bar{n}, m}{p}\right),$$
$$\left(\frac{N_1, m}{p}\right) = \left(\frac{n(\beta), m}{p}\right)\left(\frac{\bar{n}_1, m}{p}\right) = \left(\frac{\bar{n}_1, m}{p}\right),$$

et comme

$$\left(\frac{\bar{n}, m}{p}\right) = \left(\frac{\bar{n}_1, m}{p}\right)$$

pour $p = l_1 \dots l_r$. Le théorème est donc démontré.

29. La répartition des classes d'idéaux en genres. — Nous réunirons, en un même groupe, toutes les classes d'idéaux possédant le même système de caractères, et nous dirons que toutes ces classes appartiennent à un même *genre.* Le genre qui contient la classe principale est le *genre principal.* Son système de caractères est composé d'unités toutes positives.

Théorème. — Chacun des genres du corps $k(\sqrt{m})$ contient le même nombre de classes.

Démonstration : Soient $H_1, H_2 \ldots H_f$ les classes du genre principal, et soit K une classe qui n'appartient pas à ce genre, alors 1° les classes $KH_1, KH_2 \ldots KH_f$ sont toutes différentes, et 2° elles appartiennent au même genre.

En effet, soient $\mathfrak{j}, \mathfrak{h}_1, \mathfrak{h}_2 \ldots \mathfrak{h}_f$ des idéaux appartenant respectivement à K, $H_1 \ldots H_f$, on ne peut avoir

$$\mathfrak{j}\mathfrak{h}_1 \sim \mathfrak{j}\mathfrak{h}_2 \quad \text{sans quoi on aurait} \quad \mathfrak{h}_1 \sim \mathfrak{h}_2,$$

on a donc aussi $KH_1 \neq KH_2$.

On a de plus

$$\left(\frac{\pm n(\mathfrak{j}\mathfrak{h}_1).m}{l_i}\right) = \left(\frac{\pm n(\mathfrak{j}).n(\mathfrak{h}_1).m}{l_i}\right) = \left(\frac{\pm n(\mathfrak{j}_1).m}{l_i}\right)\left(\frac{\pm n(\mathfrak{h}_1).m}{l_i}\right).$$

et de même pour $\mathfrak{h}_2, \mathfrak{h}_3 \ldots \mathfrak{h}_f$. Toutes les classes $KH_1 \ldots KH_f$ ont donc le même système de caractères.

Soit L une classe qui n'est pas comprise dans les précédentes, le système des caractères de L ne peut être ni celui de la classe principale ni celui des classes $KH_1 \ldots KH_f$.

Soit $\mathfrak{l}$ un idéal de la classe L et $\mathfrak{j}$ un idéal de la classe K (et aussi de KH_1, si H_1 est la classe principale). Soit (i) un idéal principal, divisible par $\mathfrak{j}^1$, il existe un idéal $\mathfrak{a}$, tel que

$$(i)\mathfrak{l} = \mathfrak{j}.\mathfrak{a}.$$

et on a

$$\left(\frac{\pm n(i\mathfrak{l}).m}{l_i}\right) = \left(\frac{\pm n(\mathfrak{l}).m}{l_i}\right).$$

$$\left(\frac{\pm n(\mathfrak{l}).m}{l_i}\right) = \left(\frac{\pm n(\mathfrak{j}).m}{l_i}\right)\left(\frac{\pm n(\mathfrak{a}).m}{l_i}\right)$$

pour

$$i = 1, 2 \ldots r.$$

Si L admettait le même système de caractères que K ou que KH_s, on aurait

$$\left(\frac{\pm n(\mathfrak{a}), m}{l_i}\right) = +1$$

pour $i = 1, \ldots r$. Mais alors $\mathfrak{a}$ appartiendrait à une classe du genre principal, et on aurait

$$L = KH_s.$$

L serait donc une des classes déjà considérées.

Les classes $KH_1 \ldots KH_f$, et celles-là seulement, appartiennent à un même genre. On démontrera le même fait, et de la même manière pour

$$LH_1 \ldots LH_f.$$

il est évident qu'en continuant ainsi, on épuisera toutes les classes d'idéaux. Le théorème est démontré.

On peut déjà tirer de là des conséquences importantes.

Lorsque le discriminant d'un corps $k(\sqrt{m})$ ne contient qu'un seul nombre premier, le nombre des classes d'idéaux est impair, et le système des caractères d'une classe n'est composé que d'une unité, soit $+1$, soit -1. Il ne pourrait donc y avoir que deux genres, mais comme le nombre des classes du corps est impair, toutes les classes appartiennent à un seul et même genre, dont le système des caractères est, soit $+1$, soit -1.

Théorème. — Soient n et m deux entiers rationnels sans facteurs carrés

$$\prod_p \left(\frac{n, m}{p}\right) = +1,$$

où le produit Π s'étend à tous les nombres premiers rationnels.

Démonstration : Tout d'abord, pour tout nombre premier p qui ne divise ni n ni m

$$\prod_p \left(\frac{n, m}{p}\right) = +1.$$

Si n et m sont deux nombres impairs positifs et sans diviseur commun, il ne nous reste donc plus qu'à considérer dans

$$\prod_p \left(\frac{n,\,m}{p}\right),$$

en plus de $p = 2$, les nombres premiers p, facteurs de n ou de m, ce qui nous donne

$$\prod_p \left(\frac{n,\,m}{p}\right) = \left(\frac{n,\,m}{2}\right)\left(\frac{n}{p_1}\right)\cdots\left(\frac{n}{p_\mu}\right)\left(\frac{m}{q_1}\right)\cdots\left(\frac{m}{q_\nu}\right).$$

Mais d'après la loi de réciprocité, généralisée par Jacobi

$$\left(\frac{n}{m}\right)\left(\frac{m}{n}\right) = \left(\frac{n}{p_1}\right)\cdots\left(\frac{n}{p_\mu}\right)\left(\frac{m}{q_1}\right)\cdots\left(\frac{m}{q_\nu}\right) = (-1)^{\frac{n-1}{2}\cdot\frac{m-1}{2}},$$

et comme d'autre part

$$\left(\frac{n,\,m}{2}\right) = (-1)^{\frac{n-1}{2}\cdot\frac{m-1}{2}},$$

on voit que

$$\prod_p \left(\frac{n,\,m}{p}\right) = (-1)^{\frac{n-1}{2}\cdot\frac{m-1}{2}}(-1)^{\frac{n-1}{2}\cdot\frac{m-1}{2}} = +1.$$

Soient encore m et n deux entiers impairs sans facteur commun, m positif, n négatif $= -n_1$

$$\prod_p \left(\frac{n,\,m}{p}\right) = \prod\left(\frac{-n_1,\,m}{p}\right) = \prod\left(\frac{-1,\,m}{p}\right)\prod\left(\frac{n,\,m}{p}\right),$$

le second facteur est égal à 1. Le premier

$$\prod_p \left(\frac{-1,\,m}{p}\right) = \left(\frac{-1,\,m}{2}\right)\left(\frac{-1}{m}\right),$$

$$\left(\frac{-1,\,m}{2}\right) = (-1)^{\frac{m-1}{2}}, \quad \left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}},$$

par conséquent

$$\prod\left(\frac{n,\,m}{p}\right) = +1.$$

Si n est positif et m négatif $= -m_1$,

$$\prod_p \left(\frac{n, -m_1}{p}\right) = \prod_p \left(\frac{-m_1, n}{p}\right) = +1.$$

Soient de plus n, m deux nombres impairs, qui n'ont qu'un facteur premier commun r, $m = rm_1$, $n = rn_1$,

$$\prod_p \left(\frac{n_1, m}{p}\right) = \left(\frac{m_1, n}{2}\right) \left(\frac{-m_1, n_1}{r}\right) \left(\frac{n}{m_1}\right) \left(\frac{m}{n_1}\right) = +1.$$

On résout de même le cas où n, m ont plusieurs facteurs premiers communs $r, s \ldots.$ Il ne reste plus qu'à considérer les cas où 2 entre comme facteur dans l'un des nombres, ou dans chacun d'eux.

Soit d'abord m impair et n pair, $n = 2n_1$, on a

$$\prod_p \left(\frac{2n_1, m}{p}\right) = \prod_p \left(\frac{2, m}{p}\right) \prod_p \left(\frac{n_1, m}{p}\right) = \prod_p \left(\frac{2, m}{p}\right),$$

mais

$$\prod_p \left(\frac{2, m}{p}\right) = \left(\frac{2, m}{2}\right) \cdot \left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}} \cdot (-1)^{\frac{m^2-1}{8}} = +1,$$

donc

$$\prod_p \left(\frac{2n_1, m}{p}\right) = +1.$$

Soit n impair et m pair, $m = 2m_1$,

$$\left(\frac{n, m}{p}\right) = \left(\frac{m, n}{p}\right),$$

ou, on a encore

$$\prod_p \left(\frac{n, 2m_1}{p}\right) = +1.$$

Soit enfin $n = 2n_1$, $m = 2m_1$,

$$\prod_p \left(\frac{2n_1, 2m_1}{p}\right) = \prod_p \left(\frac{2, 2m_1}{p}\right) \prod_p \left(\frac{n_1, 2m_1}{p}\right) = \prod_p \left(\frac{2, 2m^1}{p}\right).$$

$$\prod_p \left(\frac{2, 2m_1}{p}\right) = \prod_p \left(\frac{2, 2}{p}\right) \prod_p \left(\frac{2, m_1}{p}\right) = \prod_p \left(\frac{2, 2}{p}\right).$$

Il suffit de connaître $\left(\frac{2,\ 2}{2}\right)$, car pour toutes les autres valeurs de p on a

$$\left(\frac{2,\ 2}{p}\right) = +1.$$

Mais dans le corps $k(\sqrt{2})$, 2 est la norme de $2 + \sqrt{2}$, c'est-à-dire

$$\left(\frac{2,\ 2}{2}\right) = +1.$$

donc on a

$$\prod\left(\frac{2n_1,\ 2m_1}{p}\right) = +1.$$

le théorème est complètement démontré.

Il est vrai, qu'à la condition que l'un des nombres n, m, au moins, soit positif. Si n et m sont négatifs, $n = -n_1$, $m = -m_1$,

$$\prod_p\left(\frac{-n_1,\ -m_1}{p}\right) = \prod_p\left(\frac{-1,\ -m_1}{p}\right)\prod_p\left(\frac{n_1,\ -m_1}{p}\right)$$
$$= \prod_p\left(\frac{-1,\ -1}{p}\right)\prod_p\left(\frac{-1,\ m_1}{p}\right) = \left(\frac{-1,\ -1}{2}\right).$$

Mais

$$\left(\frac{-1,\ -1}{2}\right) = -1$$

pour m et n négatifs,

$$\prod_p\left(\frac{n,\ m}{p}\right) = -1.$$

Le théorème précédent nous permet de faire une remarque qui est fondamentale dans l'étude des genres.

Soit $n(\mathfrak{j})$ la norme d'un idéal du corps $k(\sqrt{m})$, la définition des systèmes de caractère de l'idéal $\mathfrak{j}$, nous montre que la norme $\bar{n} = n(\mathfrak{j})$ doit toujours être prise positivement pour m négatif, c'est-à-dire que lorsqu'on considère $\bar{n}$ et m, la condition que l'un des nombres au moins est positif, est toujours remplie.

Soit $\bar{n} = \pm n(\mathfrak{j})$ la norme d'un idéal non principal, on peut poser

$$1 = \prod_p \left(\frac{\bar{n}, m}{p}\right) = \prod{}' \left(\frac{\bar{n}, m}{p}\right),$$

où le produit Π' ne s'étend qu'aux facteurs premiers de $\bar{n}$ et de m, et (à $p = 2$, lorsque m et $\bar{n}$ sont impairs).

Désignons par $q_1, q_2 \ldots q_\nu$ les facteurs premiers impairs de $\bar{n}$, qui ne divisent pas m, on a par suite de l'hypothèse

$$\left(\frac{m}{q_1}\right) = +1, \quad \left(\frac{m}{q_2}\right) = +1, \ldots \quad \left(\frac{m}{q_\nu}\right) = +1,$$

et il reste

$$\overline{\prod_p} \left(\frac{\bar{n}, m}{p}\right) = +1,$$

où le produit $\overline{\Pi}$ ne s'étend qu'aux facteurs premiers de m et aussi dans certains cas à $p = 2$.

Si donc $\Pi''\left(\frac{\bar{n}, m}{p}\right)$ qui s'étend à tous les facteurs premiers p du discriminant du corps $k(\sqrt{m})$, on voit que

$$\prod_p{}'' \left(\frac{\bar{n}, m}{p}\right) = +1$$

pour $m \equiv 3\ (4)$, $m \equiv 2\ (4)$.

D'autre part, si $m \equiv 1\ (4)$, on a avec les mêmes notations

$$1 = \overline{\prod_p} \left(\frac{\bar{n}, m}{p}\right) = \left(\frac{\bar{n}, m}{2}\right) \prod_p{}'' \left(\frac{\bar{n}, m}{p}\right).$$

Le nombre $\bar{n}$ (pris comme norme d'un idéal) ne peut contenir le facteur 2, que si 2 se décompose dans $k(\sqrt{m})$, c'est-à-dire lorsque $m \equiv 1\ (8)$. En tenant compte des formules établies pour $\left(\frac{\bar{n}, m}{2}\right)$, on obtient que $\bar{n}$ soit pair ou impair,

$$\prod_p{}'' \left(\frac{\bar{n}, m}{p}\right) = +1.$$

Si, de plus, on considère que le système des caractères d'un idéal principal ne contient que des unités positives, et si l'on remarque que H' contient le produit de tous les $\left(\frac{\bar{n}, n}{p}\right)$ qui forme le système des caractères de $\mathfrak{j}$, on peut résumer ainsi les résultats précédents.

Théorème. — Le produit des r unités d'un système de caractères d'un idéal quelconque est toujours égal à 1. Ou encore : un système de r unités ± 1 ne peut représenter un système de caractères d'un idéal du corps, que si le produit de ces r unités $= + 1$.

On peut imaginer 2^n, combinaisons de n unités ± 1. Pour $e = 1$, on a $\left\{\begin{matrix} +1 \\ -1 \end{matrix}\right.$. Soit N le nombre des combinaisons pour e unités, pour $e + 1$ unités on aura N en ajoutant $+ 1$, et N autres en ajoutant $- 1$, c'est-à-dire $2 . \mathrm{N}$ combinaisons, donc pour n unités, 2^n combinaisons.

Soit N_1 le nombre des combinaisons de e unités, contenant un nombre pair d'unités négatives, N_2 le nombre de celles qui en contiennent un nombre impair, on a $\mathrm{N}_1 + \mathrm{N}_2 = \mathrm{N}$. Passons à $2 + 1$ unités, le nombre des combinaisons contenant un nombre pair d'unités négatives sera $\mathrm{N}_1 + \mathrm{N}_2$, et celui des combinaisons en contenant un nombre impair sera également $\mathrm{N}_1 + \mathrm{N}_2$. Dans les premières combinaisons le produit des unités $= + 1$, le produit dans les secondes $= - 1$.

On voit donc qu'avec r unités $= \pm 1$ on peut former 2^{r-1} combinaisons de r unités, dont le produit $= + 1$, et ces combinaisons seules sont possibles comme système de caractères de tous les genres possibles, d'où :

Théorème. — Un corps quadratique $k(\sqrt{m})$ contient au plus 2^{r-1} genres différents.

Il s'agit de savoir si ces 2^{r-1} genres existent réellement ; pour le démontrer, nous étudierons d'abord avec soin les classes ambiges du corps.

30. Les classes ambiges. — En général deux idéaux conjugués $\mathfrak{a}$ et $\mathfrak{a}'$, d'un corps quadratique, déterminent, deux classes différentes (réciproques) du corps. Les classes particulières qui, comme la classe principale, contiennent à la fois un idéal $\mathfrak{a}$ et son conjugué $\mathfrak{a}'$, sont dites des *classes ambiges*.

Tout idéal $\mathfrak{j}$, d'une classe ambige, est donc équivalent à son conjugué, c'est-à-dire que

$$\mathfrak{j} \sim \mathfrak{j}'.$$

Le carré A^2, d'une classe ambige A, est toujours la classe principale, et quand le carré d'une classe est la classe principale, cette classe est ambige.

Il est évident que toutes les classes qui contiennent des idéaux ambiges sont ambiges, mais on peut imaginer qu'il y a des classes ambiges qui ne contiennent pas d'idéaux ambiges.

Pour trouver le nombre de classes ambiges, distinctes du corps, nous compterons d'abord les classes distinctes contenant des idéaux ambiges, puis nous ajouterons le nombre des classes ambiges qui ne contiennent pas d'idéal ambige.

D'après le théorème concernant les diviseurs idéaux du discriminant du corps, tout nombre premier qui divise le discriminant est le carré d'un idéal premier. Soient donc l_1, ... l_t tous les facteurs premiers différents du discriminant, et $\mathfrak{l}_1$, $\mathfrak{l}_2$ ... $\mathfrak{l}_t$ les diviseurs premiers idéaux de ces diviseurs premiers, on a là t idéaux ambiges distincts.

Les produits deux à deux, trois à trois, etc., de ces idéaux premiers, sont encore des idéaux ambiges, et comme abstraction faite du produit de tous ces idéaux $\mathfrak{l}_i$ qui est égal à $\sqrt{m}$, on a

$$2^t - 1,$$

en tenant compte des idéaux eux-mêmes, le corps quadratique contient $2^t - 1$ idéaux ambiges, c'est-à-dire 2^t en y comptant l'idéal (1).

M. Hilbert, voulant établir le nombre de classes distinctes, a tout d'abord introduit la notion suivante :

Définition : Un système de classes ambiges est dit un système de classes ambiges *indépendantes*, lorsqu'aucune de ces classes ne peut être exprimée par un produit de puissances d'autres classes du système, et lorsqu'aucune de ces classes n'est la classe principale.

En ce qui concerne les classes indépendantes, provenant des idéaux premiers ambiges du corps, on a le théorème fondamental.

Théorème. — Les t idéaux premiers ambiges, qui divisent le discriminant d'un corps quadratique $k(\sqrt{m})$, déterminent :

1° $t - 1$, classes ambiges indépendantes, dans le cas d'un corps imaginaire ;

2° Ils en déterminent $t - 2$ ou $t - 1$, dans le cas d'un corps réel, suivant que la norme de l'unité fondamentale est $+1$ ou -1.

Suivant les cas, le corps contient 2^{t-1}, 2^{t-2} ou 2^{t-1}, classes ambiges distinctes avec des idéaux ambiges.

Démonstration : 1. Supposons d'abord que $k(\sqrt{m})$ représente un corps imaginaire.

Pour $k(\sqrt{-1})$,

$$d = -4, \quad t_1 = 2, \quad t = 1,$$

le seul idéal ambige du corps est

$$\mathfrak{j}_1 = (1 + \sqrt{-1}) \sim 1,$$

il y a une classe ambige, la classe principale.

Pour $k(\sqrt{-2})$,

$$d = 8, \quad t_1 = 2, \quad t = 1,$$

et comme

$$\mathfrak{j}_1 = (\sqrt{-2}) \sim 1,$$

il n'y a pas de classe ambige indépendante.

On a le même résultat pour $k(\sqrt{-3})$.

Les deux corps $k(\sqrt{-1})$ et $k(\sqrt{-2})$ sont les seuls corps imaginaires qui admettent des unités différentes de ± 1. Pour tout corps imaginaire, tel que $|m| > 3$, ± 1 sont les seules unités.

Soit $(\alpha) = (x + y\omega)$ un idéal principal ambige du corps imaginaire $k(\sqrt{m})$, il faut que

$$x + y\omega = \pm(x + y\omega'),$$

c'est-à-dire si $|m| > 3$, on a ou

1) $$x + y\omega = x + y\omega'$$

ou

2) $$x + y\omega = -x - y\omega'.$$

L'égalité (1) n'admet d'autre solution que $y = 0$ et $x = a$, un nombre entier rationnel quelconque.

Par contre, l'égalité (2) nous donne

1. pour $\omega = \sqrt{m}$, $x = 0$, $y = b$ et en particulier $y = 1$,

2. pour $\omega = \frac{1 + \sqrt{m}}{2}$, $x = -b$, $y = 2b$,

d'où il résulte que (1) et $(\sqrt{m})$ sont les seuls idéaux principaux ambiges du corps.

Si $m \equiv 1$ (4) ou $m \equiv 2$ (4), le produit de tous les idéaux ambiges du corps

$$\mathfrak{l}_1 \mathfrak{l}_2 \ldots \mathfrak{l}_t = (\sqrt{m});$$

si $m \equiv 3$ (4), et si $\mathfrak{l}_1$ désigne l'idéal premier ambige contenu dans (2), on a

$$\mathfrak{l}_2 \mathfrak{l}_3 \ldots \mathfrak{l}_t = (\sqrt{m}).$$

Dans les deux cas, l'un des idéaux contenus dans $(\sqrt{m})$, par exemple $\mathfrak{l}_t$, peut être exprimé au moyen des autres et de $(\sqrt{m})$, de telle sorte qu'on obtient au plus $t - 1$ classes ambiges indépendantes.

On ne peut peut d'ailleurs avoir

$$\mathfrak{l}_1 \sim \mathfrak{l}_2 \mathfrak{l}_3 \ldots \mathfrak{l}_\nu,$$

lorsque $m \equiv 1$ ou $m \equiv (2)$ (4), ou

$$\mathfrak{l}_2 \sim \mathfrak{l}_3 \mathfrak{l}_4 \ldots \mathfrak{l}_\nu,$$

quand $m \equiv 3$ (4) pour $\nu \leqq t - 1$, car on aurait alors

$$\mathfrak{l}_1 \mathfrak{l}_2 \ldots \mathfrak{l}_\nu \sim 1,$$

ou

$$\mathfrak{l}_2 \ldots \mathfrak{l}_\nu \sim 1,$$

ce qui n'est pas possible, étant donnée la remarque faite au début. Par conséquent les $t - 1$ idéaux $\mathfrak{l}_1$, $\mathfrak{l}_2$, ... $\mathfrak{l}_{t-1}$ engendrent $t - 1$, classes ambiges indépendantes.

Si de plus l'on forme les produits des $t - 1$ idéaux $\mathfrak{l}_1 - \mathfrak{l}_{t+1}$, 2 à 2, 3 à 3, etc., il en résulte un système de $2^{t-1} - 1$ idéaux ambiges, parmi lesquels il n'y a aucun idéal principal et tels qu'il

n'y ait pas deux qui soient équivalents ; il y a donc dans le corps 2^{t-1}, classes qui contiennent des idéaux ambiges.

2. Soit $k(\sqrt{m})$ au corps réel. Les corps réels se comportent de manières différentes, suivant que l'unité fondamentale $\varepsilon = + 1$ ou $= - 1$. Dans le premier cas $n(\varepsilon) = + 1$, il y a toujours dans le corps $k(\sqrt{m})$ un nombre entier différent de 1 et de $\pm \sqrt{m}$ tel que $\varepsilon = \frac{\alpha}{\alpha'}$. De $\varepsilon = \frac{\alpha}{\alpha'}$ résulte

$$(\alpha) = (\alpha'),$$

et (α) représente un idéal différent de (1) et de $(\sqrt{m})$. Il n'existe pas dans le corps outre (1) $(\sqrt{m})$ (α), et peut-être de l'idéal $(\sqrt{m}\alpha)$ débarrassé de ses facteurs rationnels, qui soit indépendant des précédents.

Car soit (β) un idéal principal ambige du corps, il existe un nombre f tel que $\beta = \pm \varepsilon^f \beta'$, mais comme $\alpha' = \varepsilon^f \alpha'$, le quotient

$$(1) \qquad \gamma = \frac{\beta}{\alpha'} \quad \text{dans le cas où } \beta = + \varepsilon^f \beta',$$

$$(2) \qquad \gamma = \frac{\beta}{\sqrt{m}\alpha'} \quad \text{dans le cas où } \beta = - \varepsilon^f \beta',$$

est un nombre pour lequel $\frac{\gamma}{\gamma'} = + 1$. Ceci n'est possible que si γ est un nombre rationnel, il n'y a donc pas à part (1), $(\sqrt{m})$, (α), et $(\sqrt{m}\alpha)$ débarrassé de ses facteurs rationnels d'autre idéal principal ambige indépendant de ces idéaux.

En deuxième lieu si l'unité fondamentale a pour norme $n(\varepsilon) = - 1$, le corps quadratique n'admet que (1) et $(\sqrt{m})$ comme idéaux principaux ambiges.

Car soit (α) un idéal ambige principal différent de (1) et de $(\sqrt{m})$ et qui n'est pas divisible par $(\sqrt{m})$, on pose

$$\frac{\alpha}{\alpha'} = \pm \varepsilon^{f'},$$

de là il résulte $n(\pm \varepsilon') = +1$, et l'exposant f est pair, car $n(\varepsilon) = -1$. Soit alors

$$(1) \quad \beta = \frac{\alpha}{\varepsilon^{\frac{f}{2}}} \quad \left\{ \begin{array}{l} \text{dans le cas où} \quad f \equiv 0 \ (2) \quad \text{et} \quad \frac{\alpha}{\alpha'} = +\varepsilon^f, \\ \text{ou dans le cas} \quad f \equiv 1 \ (2) \quad \text{et} \quad \frac{\alpha}{\alpha'} = -\varepsilon^f, \end{array} \right.$$

$$(2) \quad \beta = \frac{\alpha}{\sqrt{m}\,\varepsilon^{\frac{f}{2}}} \quad \left\{ \begin{array}{ll} f \text{ pair}, & \frac{\alpha}{\alpha'} = -\varepsilon^f, \\ f \text{ impair}, & \frac{\alpha}{\alpha'} = +\varepsilon^f, \end{array} \right.$$

β est un nombre entier tel que $\frac{\beta}{\beta'} = +1$, β est un nombre rationnel, c'est-à-dire que

$$(\alpha) = (1) \quad \text{et} \quad (\alpha) = (\sqrt{m})$$

sont les seuls idéaux principaux ambiges.

Les idéaux principaux ambiges d'un corps réel étant connus, on obtient comme précédemment le système des idéaux ambiges non équivalents et les classes ambiges indépendantes.

Lorsque le corps réel a pour norme $n(\varepsilon) = -1$, parmi les t idéaux premiers $\mathfrak{l}_1 \ldots \mathfrak{l}_t$, il y en a qui s'expriment au moyen de $\sqrt{m}$ et des autres, mais lorsque $n(\varepsilon) = +1$ il y a deux des idéaux premiers ambiges diviseurs de $\sqrt{m}$ ou de α qui s'expriment au moyen de $\sqrt{m}$ et de α et des autres.

On obtient donc $t - 1$ ou $t - 2$ classes ambiges indépendantes, suivant les cas.

Pour achever la solution de la question des classes ambiges, il nous faut encore savoir s'il existe dans le corps des classes ambiges qui ne contiennent pas d'idéal ambige, et à déterminer leur nombre.

Soit un idéal non ambige d'une classe ambige du corps $k(\sqrt{m})$, et soit γ un nombre tel que

$$(\gamma)\mathfrak{j} = \mathfrak{j}',$$

et que de plus

$$n(\gamma) = +1,$$

la classe contient certainement un idéal ambige, car comme $n(\gamma) = 1$, il y a dans le corps k un nombre entier β, tel que

$$\gamma = \frac{\beta}{\beta'},$$

et par suite

$$(\beta)\mathfrak{j} = (\beta')\mathfrak{j}'$$

$(\beta)\mathfrak{j}$ est donc lui-même un idéal ambige, ou le produit d'un idéal ambige par des facteurs rationnels.

On ne peut donc avoir une classe ambige sans idéal ambige, que si $(\gamma)\mathfrak{j} = \mathfrak{j}'$ avec $n(\gamma) = -1$. Ceci n'est possible que pour des corps réels. Si dans un corps réel on avait $n(\gamma) = -1$, l'unité fondamentale étant égale à -1, on aurait

$$n(\varepsilon\gamma) = +1.$$

et l'on pourrait poser

$$\varepsilon\gamma = \frac{\beta}{\beta'}.$$

de sorte qu'on aurait à nouveau $(\beta)\mathfrak{j} = (\beta')\mathfrak{j}'$, la classe contiendrait donc un idéal ambige.

Ces remarques faites, nous allons démontrer :

Théorème. — La condition nécessaire et suffisante pour que le corps quadratique $k(\sqrt{m})$ contienne une classe ambige ne possédant pas d'idéal ambige est que le système de caractères de -1 ne soit composé que d'unités positives, et que la norme de l'unité fondamentale ε soit $+1$.

On obtient alors toutes les classes de cette espèce, en multipliant l'une d'entre elles successivement par chacune des classes ambiges qui possèdent des idéaux ambiges.

Démonstration : En vertu des théorèmes sur les restes normiques, le système des caractères de -1 ne contient que des unités positives, lorsque -1 est la norme d'un nombre entier ou fractionnaire du corps. Réciproquement, si le système de caractères de -1 ne contient que des unités positives, tous les facteurs premiers rationnels de m, sauf le facteur possible 2, sont de la forme $4n + 1$, et m est la somme de deux carrés

$$m = u^2 + v^2,$$

c'est-à-dire

$$-1 = \frac{u^2 - m}{v^2},$$

et l'on voit que — 1 est la norme d'un nombre entier ou fractionnaire du corps $k(\sqrt{m})$. Ce nombre est nécessairement fractionnaire, s'il était entier il serait une unité, et d'après l'hypothèse, les normes des unités sont égales à + 1.

Soit alors γ un nombre fractionnaire de la forme $n(\gamma) = -1$, mettons γ sous la forme de deux idéaux premiers entre eux,

$$\gamma = \frac{\mathfrak{j}}{\mathfrak{j}_1} \quad \text{ou} \quad \mathfrak{j} = (\gamma)\mathfrak{j}_1,$$

comme $n(\gamma) = -1$,

$$\mathfrak{j}\mathfrak{j}' = \mathfrak{j}_1\mathfrak{j}_1'.$$

Comme $\mathfrak{j}$ et $\mathfrak{j}_1$ sont premiers entre eux, il en est de même de $\mathfrak{j}'$ et de $\mathfrak{j}_1'$, et par suite $\mathfrak{j} = \mathfrak{j}_1'$, donc $\mathfrak{j}' \sim \mathfrak{j}$, et $\mathfrak{j}$ détermine une classe ambige. Cette classe ne peut contenir aucun idéal ambige, sans quoi on aurait $n(\gamma) = +1$, ce qui n'est pas le cas et ce qui n'a pas lieu non plus pour $\varepsilon\gamma$, car $n(\varepsilon) = +1$.

La première partie du théorème est donc démontrée.

Soit $\mathfrak{j}$ un idéal qui n'est pas ambige, mais qui détermine une classe ambige, et soient $\mathfrak{a}_1$, $\mathfrak{a}_2$, ... des idéaux ambiges appartenant aux différentes classes ambiges trouvées antérieurement, les idéaux

$$\mathfrak{j}\mathfrak{a}_1, \ \mathfrak{j}\mathfrak{a}_2, \ \ldots$$

déterminent : 1° des classes toutes différentes ; 2° ils déterminent toutes les classes qui ne contiennent pas d'idéal ambige.

Tout d'abord si l'on avait

$$\mathfrak{j}\mathfrak{a}_\nu \sim \mathfrak{j}\mathfrak{a}_\mu,$$

on aurait

$$\mathfrak{a}_\nu \sim \mathfrak{a}_\mu,$$

ce qui est contraire à l'hypothèse.

Soit de plus $\mathfrak{J}$ un idéal non ambige appartenant à l'une des classes ambiges que nous cherchons, et supposons que $\mathfrak{j}$ appar-

tienne pas à cette classe. Il y a dans le corps deux nombres γ et γ_1, tels que

$$n(\gamma) = n(\gamma_1) = -1$$

et

$$\frac{\mathfrak{j}}{\mathfrak{j}'} = \gamma, \quad \frac{\mathfrak{J}}{\mathfrak{J}'} = \gamma_1,$$

c'est-à-dire

$$\frac{\mathfrak{j}\mathfrak{J}}{\mathfrak{j}'\mathfrak{J}'} = \gamma\gamma_1,$$

mais comme $n(\gamma\gamma_1) = +1$, $\gamma\gamma_1 = \frac{\alpha}{\alpha'}$, α étant un entier du corps, c'est-à-dire

$$\frac{\mathfrak{j}\mathfrak{J}}{\mathfrak{j}'\mathfrak{J}'} = \frac{\alpha}{\alpha'},$$

c'est-à-dire que $(\alpha)\mathfrak{j}\mathfrak{J}$ est un idéal ambige, c'est-à-dire qu'il est l'un des idéaux $\mathfrak{a}_1\mathfrak{a}_2 \ldots$, soit $(\alpha)\,\mathfrak{j}\mathfrak{J} = \mathfrak{a}$, on a

$$\mathfrak{J} \sim \mathfrak{j}'\mathfrak{a} \sim \mathfrak{j}\mathfrak{a}.$$

Toutes les classes ambiges sont donc comprises dans celles que nous avons indiquées.

[*Remarque.* — La première partie du théorème pourrait s'énoncer : m ne peut contenir d'autres facteurs que 2, et des nombres premiers de la forme $4n+1$. Nous l'avons rattaché plus étroitement à la définition des systèmes de caractères].

Nous arrivons maintenant au

Théorème. — Tout corps quadratique contient 2^{t-1} classes ambiges différentes.

Démonstration : 1. Le corps est imaginaire, alors $r = t$, toute classe ambige contient nécessairement un idéal ambige, le nombre total des classes ambiges est donc

$$2^{t-1} = 2^{r-1}.$$

2. Le corps est réel, on a trois cas à distinguer suivant le système des caractères de -1 et suivant la valeur de l'unité fondamentale.

a) Le système des caractères de -1 contient au moins une

fois — 1. Dans ce cas $r = t - 1$. La norme de l'unité fondamentale $= + 1$. Toute classe ambige contient au moins un idéal ambige et comme le nombre des classes est 2^{t-2}, 2^{r-1} est bien le nombre total des classes ambiges d'idéaux.

b) Le système des caractères de -1 ne contient que des nombres $+$, la norme de l'unité fondamentale $= -1$. Alors $r = t$. Toute classe ambige contient au moins un idéal ambige et leur nombre est

$$2^{t-1} = 2^{r-1}.$$

c) Le système des caractères de -1 ne contient que des nombres $+$, et la norme de l'unité fondamentale $= + 1$. Alors $r = t$, le corps contient 2^{t-2} classes ambiges comprenant un idéal ambige et 2^{t-2} classes ambiges ne contenant pas d'idéal ambige. Le nombre total de ces classes est 2^{r-1}.

Il est très remarquable que c'est là aussi le nombre que nous avons trouvé comme nombre maximum des genres. Il doit y avoir un rapport entre le nombre des genres et le nombre des classes ambiges, c'est ce que nous allons démontrer.

31. L'existence des genres. — *Théorème.* — Si le symbole $\left(\frac{n, m}{p}\right) = + 1$ pour les nombres n et m qui ne contiennent aucun facteur carré quel que soit le nombre p, n est la norme d'un nombre entier ou fractionnaire du corps $k(\sqrt{m})$.

Démonstration : Si $\left(\frac{n, m}{p}\right) = + 1$ pour tous les nombres premiers p, l'un des nombres n et m au moins est positif.

Si m est négatif n est positif, ce qui d'ailleurs est une condition nécessaire pour que n soit la norme d'un nombre du corps imaginaire $k(\sqrt{m})$. Si m est positif n peut être négatif ou positif.

L'hypothèse exige que n soit la norme ou d'un nombre entier du corps ou d'un idéal appartenant au genre principal, car pour tout facteur premier impair q de n qui ne divise pas m, on a $\left(\frac{m}{p}\right) = + 1$, et pour tout facteur premier impair q de n qui divise m $\left(\frac{m}{q}\right) = 0$, c'est-à-dire que n se décompose dans le corps $k(\sqrt{m})$. Remarquons

de plus que si n est pair $n = 2n_1$, 2 se décompose pour $m \equiv 2$, $m \equiv 3\ (4)$, et que pour $m \equiv 1\ (4)$ 2 ne se décompose que si

$$\left(\frac{2n_1, m}{2}\right) = (-1)^{\frac{m^2-1}{8}} = +1,$$

et si 2 se décompose dans $k(\sqrt{m})$.

Posons donc $n = \pm\, n(\mathfrak{j})$ où $\mathfrak{j}$ est un idéal du corps.

Mais il résulte du théorème fondamental établi au n° 16, que l'on peut choisir un idéal $\mathfrak{h}$ de la classe de $\mathfrak{j}$ tel que $n(\mathfrak{h}) = n_1$ avec $|n_1| < |\sqrt{d}|$; α étant un nombre entier ou fractionnaire, on a :

$$\mathfrak{j} = \alpha\, \mathfrak{h},$$

$$n = \pm\, n(\mathfrak{j}) = \pm\, n(\alpha)\, n(\mathfrak{h}) = n(\alpha)\,.\, n_1.$$

Si $n_1 = 1$, le théorème est démontré, sinon dans ce qui suit nous pouvons admettre que n_1 est un entier rationnel sans factenr carré, pour lequel

$$\left(\frac{n_1, m}{p}\right) = +1,$$

pour toutes les valeurs de p, c'est-à-dire que notre théorème sera démontré pour toutes les valeurs de n_1 lorsque nous aurons démontré qu'il est vrai pour m quelconque, et n_1 tel que $|n_1| \leqq |\sqrt{d}|$.

Si le théorème est vrai pour n_1 et m cela veut dire que

$$n_1 = \frac{x^2 - my^2}{u^2 - mv^2},$$

x, y ne pouvant être nuls à la fois, pas plus que u et v ; ni non plus x et u, y et v, dans ce dernier cas, n_1 serait un carré.

On peut donc résoudre par rapport à m, et écrire

$$m = \frac{x^2 - n_1 u^2}{y^2 - n_1 v^2}.$$

Mais

$$\left(\frac{n_1, m}{p}\right) = \left(\frac{m, n_1}{p}\right).$$

Si donc le théorème est vrai pour n_1 et m, il est vrai aussi pour m et n_1 ou $|n_1| \leqq |\sqrt{d}|$.

Si $|m| > 4$, $|\sqrt{d}| < |m|$ et par suite aussi $|n_1| < |m|$.

D'après ce qui précède : étant donnés deux nombres m et n, on peut toujours ramener le cas général au cas de deux nouveaux nombres $\overline{n} = m_1$, $\overline{m} = n_1$, qui sont inférieurs en valeur absolue à $|m|$ tant que $|\sqrt{d_m}| < m$, c'est-à-dire tant que $|m| > 4$.

Le théorème se trouvera donc démontré d'une façon générale si nous montrons qu'il est vrai pour les corps $k(\sqrt{-1})$, $k(\sqrt{\pm 2})$, $k(\sqrt{\pm 3})$, pour lesquels $|m| < 4$.

Tous ces corps ont un nombre de classes $h = 1$. Des considérations analogues à celles que nous avons faites au début montrent que l'idéal (n) se décompose dans le corps $k(\sqrt{m})$, dans le cas où $\left(\frac{n, m}{p}\right) = +1$ pour tous les nombres premiers p. Mais alors n est la norme d'un nombre entier, car, pour les corps imaginaires, n est certainement positif. Dans le corps $k(\sqrt{-2})$ l'unité fondamentale $\varepsilon = -1$, et enfin dans le corps $k(\sqrt{-3})$, on n'a constamment $\left(\frac{n, m}{3}\right) = +1$ que si n est de la forme $\left(\frac{+n}{3}\right) = 1$, ou

$$n = 3n_1 \quad \text{avec} \quad \left(\frac{-n_1}{3}\right) = +1,$$

c'est-à-dire $+n = x^2(3)$ ou $n = x^2 - 3y^2$, et de même

$$3n_1 = 9x^2 - 3y^2.$$

Le théorème est vrai pour les corps particuliers considérés, il est donc vrai d'une façon générale. On voit de plus qu'on peut l'étendre au cas où n est quelconque.

Nous ajouterons quelques exemples :

1. Dans $k(\sqrt{-1})$,

$$\left(\frac{+1, -1}{p}\right) = +1, \quad \left(\frac{2, -1}{p}\right) = +1,$$

d'autre part

$$1 = n(-1), \quad 2 = n(1 + \sqrt{-1}).$$

2. Dans $k(\sqrt{2})$,

$$\left(\frac{\pm 1, 2}{p}\right) = +1 \quad \text{et} \quad -1 = n(\varepsilon),$$

où $\varepsilon = 1 + \sqrt{2}$ est l'unité fondamentale des corps,

$$\left(\frac{\pm 2, 2}{p}\right) = +1, \quad 2 = n[\sqrt{2}(1 + \sqrt{2})],$$
$$-2 = n(\sqrt{2}).$$

3. Dans $k(\sqrt{-2})$,

$$\left(\frac{1, -2}{p}\right) = +1 \quad \text{et} \quad 1 = n(-1)$$
$$\left(\frac{2, -2}{p}\right) = +1, \quad 2 = n(\sqrt{-2}).$$

4. Dans $k(\sqrt{3})$,

$$\left(\frac{1, 3}{p}\right) = +1, \quad 1 = n(-1),$$
$$\left(\frac{-2, 3}{p}\right) = +1, \quad -2 = n(1 + \sqrt{3}).$$

5. Dans $k(\sqrt{-3})$,

$$\left(\frac{\pm 1, -3}{p}\right) = +1, \quad 1 = n(-1).$$

Dans $k(\sqrt{7})$,

$$\left(\frac{2, -7}{p}\right) = +1, \quad 2 = \frac{1}{4} + 7\frac{1}{4}.$$

On a considéré dans ces exemples tous les couples de nombres pour lesquels $|n| < |\sqrt{d_m}|$.

Théorème. — Toute classe du genre principal du corps $k(\sqrt{m})$ peut être représentée par le carré d'une classe du corps.

Démonstration : Soit $\mathfrak{h}$ un idéal appartenant à une classe du genre principal. Alors

$$\left(\frac{\pm n(\mathfrak{h}), m}{p}\right) = +1$$

pour tous les nombres premiers p. D'après le terme précédent

$$\pm n(\mathfrak{h}) = n(\alpha),$$

où α est un nombre entier ou fractionnaire du corps $k(\sqrt{m})$, posons

$$\frac{\mathfrak{h}}{(\alpha)} = \frac{\mathfrak{j}}{\mathfrak{j}_1},$$

ou $\mathfrak{j}$ et $\mathfrak{j}_1$ sont des idéaux premiers entre eux.

Si $\mathfrak{j}$ et $\mathfrak{j}_1$ sont premiers entre eux, il en est de même de leurs conjugués $\mathfrak{j}'$ et $\mathfrak{j}_1'$. Mais

$$n\left(\frac{\mathfrak{h}}{\alpha}\right) = \pm 1 = \frac{\mathfrak{j}\mathfrak{j}'}{\mathfrak{j}_1\mathfrak{j}_1'}$$

ou encore

$$\mathfrak{j}\mathfrak{j}' = \mathfrak{j}_1\mathfrak{j}_1',$$

ce qui n'est possible que si $\mathfrak{j} = \mathfrak{j}_1'$ et $\mathfrak{j}' = \mathfrak{j}_1$, c'est-à-dire que

$$\mathfrak{h} = \frac{\alpha}{n(\mathfrak{j})}\mathfrak{j}^2, \quad \text{ou encore} \quad \mathfrak{h} \sim \mathfrak{j}^2.$$

Soit H la classe de $\mathfrak{h}$, et K la classe de $\mathfrak{j}$, on a

$$H = K^2,$$

le théorème est démontré.

Nous arrivons enfin au

Théorème. — Le nombre des genres dans le corps $k\left(\sqrt{m}\right) = 2^{r-1}$.

Démonstration : Soit h le nombre des classes, g le nombre des genres, et f les nombres des classes contenues dans chaque genre. On a

$$h = g \cdot f.$$

Soient H_1H_2, ... H_f, les classes du genre principal, il y a f identités

$$H_1 = K_1^2, \ldots H_f = K_f^2$$

où K_1^2, ... K_f^2 représentent des classes différentes.

Soient A_1A_2, .., A_a les $a = 2^{r-1}$ classes ambiges du corps, on peut montrer tout d'abord que

$$\begin{matrix} K_1A_1, & K_1A_2, & \ldots & K_1A_a \\ \cdot & \cdot & \cdot & \cdot \\ K_fA_1, & K_fA_2, & \ldots & K_fA_a \end{matrix}$$

représentent toutes les classes et ne représentent chacune d'elles qu'une fois. Les classes sont bien différentes, car si l'on avait

$$K_\lambda A_\mu = K_\nu A_\rho,$$

on aurait aussi

$$K_\lambda^2 = K_\nu^2,$$

ce qui est contraire à la définition des classes K.

Soit, d'autre part, C une classe quelconque du corps, C^2 appartient certainement au genre principal et pour une certaine valeur de i :

$$C^2 = K_i^2,$$

$\frac{C}{K}$ est alors une classe ambige, et l'on peut poser $C = AK$, de sorte que C se trouve certainemeut dans le tableau précédent.

On a donc à la fois $h = gf$ et $h = af$, c'est-à-dire

$$g = 2^{r-1}.$$

On a montré précédemment que le produit des nombres d'un système de caractères est égal à $+ 1$, et qu'il y a au plus 2^{r-1} systèmes de caractères, on en conclura : dans le seul cas où la condition nécessaire et suffisante pour qu'un système de r unités $+ 1$ représente le système des caractères d'un idéal du corps, est que le produit de ces unités soit égal à 1.

Nous allons déduire de l'existence des genres quelques conséquences intéressantes.

32. Applications du théorème relatif à l'existence des genres. — 1. Lorsque le nombre des classes d'un corps est impair, toutes les classes appartiennent au même genre, car on a :

$$h = 2^{r-1}, \quad f = gf;$$

si donc h est impair, il faut que $g = 2^{r-1} = 1$.

Etudions quelques particuliers :

2. Soit $m = p$ un nombre premier positif ou négatif et soit $m \equiv 1 . (4)$; alors $d = m$, $t = 1$, $r = t = 1$, le nombre des genres est $2^0 = 1$. Le corps ne contient qu'un idéal principal ambige, et une seule classe ambige, la classe principale. Comme on

l'a vu précédemment, le nombre des classes h est impair, et si le corps est réel, l'unité fondamentale est égale à -1.

3. Soit $m = p$, un nombre positif de la forme $4n + 3$, alors $d = 4p$, $l_1 = 2$, $l_2 = p$, $t = 2$. Le système des caractères de -1 est

$$\left(\frac{-1, p}{2}\right) = -1, \quad \left(\frac{-1, p}{p}\right) = -1;$$

donc

$$r = t - 1 = 1.$$

Le nombre des classes ambiges ainsi que le nombre des genres est $2^0 = 1$.

En particulier $\mathfrak{l}_1 = (2, 1 + \sqrt{p})$ est un idéal principal, autrement dit l'équation indéterminée

$$\pm 2 = x^2 - py^2$$

admet toujours des solutions entières, et l'on peut assurer que

$$+ 2 = x^2 - py^2 \text{ en admet seule si } p = 8n + 7$$
$$- 2 = x^2 - py^2 \text{ en admet seule si } p = 8n + 3.$$

On résout en général ces équations par des essais. Souvent on y arrive plus rapidement comme dans le cas de $\pm 1 = x^2 - my^2$, en cherchant d'abord une solution de $x^2 \mp 2 \equiv 0 \ (p)$, soit w ; le nombre x se trouve parmi les nombres $x + p\lambda$, où λ est entier rationnel positif ou négatif ; il suffira de voir pour quelles valeurs de λ $\dfrac{x^2 \mp 2}{p}$, c'est-à-dire

$$\frac{w^2 \mp 2}{p} + 2w\lambda + p\lambda^2 = y^2,$$

c'est-à-dire est un carré.

4. Soit $m = -p$ un nombre premier négatif de la forme $m \equiv 3$ (4), on a $r = t = 2$. Le nombre des classes h est pair, et le corps contient deux classes ambiges avec des idéaux ambiges.

Les idéaux premiers ambiges sont $\mathfrak{a} = (\sqrt{m})$, $\mathfrak{b} = (2, 1 + \sqrt{m})$ ou $b + 1$. Si l'on pose $n(\mathfrak{a}) = \bar{n} = -m$, $n(\mathfrak{b}) = \bar{n}_1 = +2$, on obtient pour $\mathfrak{a}$ et $\mathfrak{b}$ les systèmes de caractères :

$$\left(\frac{-m, m}{2}\right) = +1, \quad \left(\frac{-m, m}{m}\right) = +1,$$

$$\left(\frac{2, m}{2}\right) = \pm 1, \quad \left(\frac{2, m}{m}\right) = \pm 1,$$

où il faut prendre les signes supérieurs ou les signes inférieurs suivant que $\pm p \equiv \left\{ \begin{smallmatrix} 1 \\ 5 \end{smallmatrix} \right. (8)$. Lorsqu'on a les deux signes $+$, la classe B appartient aussi au genre principal. Mais comme toute classe de ce genre peut être représentée par le carré d'une autre classe, on peut poser $B = K^2$, comme d'autre part $B^2 = 1$, on a aussi $K^4 = 1$, le nombre des classes du corps est divisible par 4, c'est-à-dire qu'il est au moins égal à 4.

Lorsqu'on a les deux signes —, B ne peut être le carré d'une autre classe, et le nombre des classes est divisible par 2, et non par une puissance supérieure de 2.

Désignons dans ces derniers cas par $H_1 H_2 \dots H_f$, les classes du genre principal, f étant un nombre impair, les autres classes seront

$$H_1 B,\ H_2 B,\ \dots\ H_f B,$$

et par suite de $B^2 = 1$, on a

$$H_\lambda = H_\mu^2, \qquad H_\lambda = H_\nu H_\iota,$$

où λ, μ, ν, ι, sont des nombres de la suite de 1 à f.

5. Soit $m = pp_1$ un nombre positif, et supposons que p et p_1 sont des nombres premiers positifs de la forme $4n + 1$. Alors $t = 2$, $r = t$, $g = 2^1 = 2$, le nombre des classes ambiges et des genres est 2, les idéaux ambiges sont : $(p, \sqrt{m})$; $(p_1, \sqrt{m})$; et $\sqrt{m}$; dans le cas où $n(\varepsilon) = +1$, le corps contient une classe ambige qui n'a pas d'idéal ambige, alors les trois idéaux que nous venons d'écrire sont des idéaux principaux, c'est-à-dire que

$$\pm p = \left(x + \frac{y}{2}\right)^2 - \frac{pp_1}{4} y^2,$$

$$\pm p_1 = \left(x_1 + \frac{y_1}{2}\right)^2 - \frac{pp_1}{4} y_1^2,$$

admettent des solutions entières. Soit $x + \frac{y}{2} = \frac{z}{2} p$, il en résulte que

$$\pm 1 = p\left(\frac{z}{2}\right)^2 - p_1\left(\frac{y}{2}\right)^2$$

admet des solutions entières.

Réciproquement, si ces équations admettent des solutions entières, la norme de l'unité fondamentale est $+1$.

La condition $\left(\frac{p}{p_1}\right)_{p_1} = +1$ est évidemment nécessaire pour que l'équation indéterminée ait des solutions.

D'où le

Théorème. — La norme de l'unité fondamentale du corps réel $k(\sqrt{m})$ où $m = pp_1$, pp_1 étant des nombres premiers positifs de la forme $4n+1$, est égale à -1 lorsque $\left(\frac{p}{p_1}\right) = -1$.

Lorsque $\left(\frac{p}{p_1}\right) = +1$, c'est-à-dire $\left(\frac{p_1}{p}\right) = +1$, l'unité fondamentale ε peut avoir pour norme $+1$ ou -1, ainsi qu'on le voit par les exemples $k(\sqrt{145})$ ou ($\varepsilon = 11 + 2\omega$ avec $n(\varepsilon) = -1$) et $k(\sqrt{221})$ ou ($\varepsilon = 7 + \omega$ avec $n(\varepsilon) = +1$).

Nous ne pouvons pas traiter ici le moyen de distinguer le cas où $n(\varepsilon) = +1$ et le cas où $n(\varepsilon) = -1$; mais nous ferons d'autres remarques : par exemple, lorsque $\left(\frac{p}{p_1}\right) = +1$, et que le corps $k(\sqrt{pp_1})$ a un nombre de classes égal à 2, la norme de l'unité fondamentale $= +1$.

Le résultat précédent peut encore être énoncé ainsi, des deux équations :

$$(1)\qquad \pm p = \left(x + \frac{y}{2}\right)^2 - \frac{pp_1}{4}y^2$$

ou

$$(2)\qquad \pm 1 = p\left(\frac{z}{2}\right)^2 - p_1\left(\frac{y}{2}\right)^2 ;$$

l'une, seulement, admet des solutions entières.

On a des résultats analogues pour le cas $p = 2$ et $p_1 \equiv 1\ (4)$.

6. Soit $m = qq_1$ un nombre positif dont les facteurs premiers q et q_1 sont de la forme $4n+3$. Alors $m \equiv 1\,(4)$, $t = 2$, $r = t - 1 = 1$, $g = 2^0 = 1$. Le nombre des classes est impair, car alors les idéaux ambiges sont tous des idéaux principaux, et il n'y a pas de classe ambige sans idéal ambige dans le corps. L'équivalence

$$(q, \sqrt{qq_1}) \sim 1$$

exprime que, dans tous les cas, l'une des deux équations

$$\pm 4 = qx^2 - q_1y^2$$

admet des solutions entières ou rationnelles ; c'est l'équation obtenue avec le signe +, lorsque $\left(\frac{q}{q_1}\right) = +1$; celle avec le signe — lorsque $\left(\frac{q}{q_1}\right) = -1$. [1]

7. Soit $m = \pm pq$ un entier positif ou négatif avec $p \equiv 1$, $q \equiv 3$, (4), $t = 3$ ou $= 2$, on a $r = 2$. $g = 2$; le nombre des classes est pair.

Nous résumerons les cas particuliers que nous venons d'examiner dans l'énoncé du théorème suivant : [2]

Théorème. — Le nombre des classes du corps $k(\sqrt{m})$ est impair : 1° quand m est un nombre premier positif ou négatif de la forme $m \equiv 1$ (4) ; 2° quand m est un nombre premier positif de la forme $4n + 3$; 3° quand $m = qq_1$, produit de deux nombres premiers positifs de la forme $4n + 3$.

Ce sont les seuls cas où $h = 1$. Dans tous les autres cas h est pair.

33. Les anneaux de nombres. — Nous ajoutons ici un chapitre complémentaire, pour exposer une notion très importante, et dont nous ferons une application : la notion d'*anneau de nombres* dans un *corps de nombres* [3].

Soient α, β, γ ... des nombres entiers quelconques du corps, on dit que l'ensemble formé par ces nombres, et l'ensemble de tous

---

(1) Lorsqu'on connait une solution de $\pm 4 = qx^2 - q_1y^2$, on peut, à l'aide des unités de $k(\sqrt{qq_1})$, en déterminer une infinité d'autres. On peut d'ailleurs démontrer que les équations $\pm 1 = qx^2 - q_1y^2$ admettent des solutions, suivant que $\left(\frac{q}{q_1}\right) = \pm 1$.

(2) Nous passons sous silence dans ces déductions une suite d'affirmations négatives au sujet de la non solubilité de certaines équations, etc.

(3) M. HILBERT a donné à cette notion le nom de Zahlring (*Zahlb.*, chap. IX). M. DEDEKIND, se rattachant à la nomenclature de GAUSS, le désigne par *Ordnung*. Voir *Über die Anzahl der Idealklassen in den verschiedenen Ordnungen eines endlichen Körpers, Festschr. zur Säkularf. des Geburtstages*, von GAUSS, Braunschweig, 1877. KRONECKER avait introduit l'expression *Integritätsbereich*, *Ges. Werke*, t. II.

ceux que l'on déduit de ces nombres par les opérations répétées aussi souvent que l'on veut, d'addition, de soustraction et de multiplication, ou encore toutes les fonctions entières à coefficients entiers rationnels de $\alpha, \beta, \gamma \ldots$ forment un *anneau de nombres* ou un *anneau* ou un *domaine d'intégrité*.

Il y a une infinité d'anneaux dans un corps, et le corps lui-même est le plus vaste de ces anneaux.

Soit m un nombre entier rationnel tel que $m \equiv 1 \ (4)$, on trouve comme nombre de base du corps $k(\sqrt{m})$ $\omega = \frac{1 + \sqrt{m}}{2}$. La question se pose, quelle est la différence obtenue en remplaçant le corps $k(\sqrt{m})$ par l'anneau déterminé par $1, \sqrt{m}$.

Nous désignerons cet anneau par $r(\sqrt{m})$, et comme il n'y a pas de confusion possible tout simplement par r.

On voit immédiatement :

1° Tout nombre de l'anneau r est un nombre du corps $k(\sqrt{m})$.

2° Tout nombre de l'anneau peut être mis sous la forme $a + b\sqrt{m}$, où a et b sont des nombres entiers rationnels.

Les nombres $1, \sqrt{m}$ forment une base de l'anneau.

3° Si ω_1, ω_2 et ω_1^*, ω_2^* sont deux couples de nombres de base de r, il y a quatre nombres entiers rationnels r, s, t, u, tels que

$$ru - st = \pm 1,$$

et que

$$\omega_1^* = r\omega_1 + s\omega_2,$$
$$\omega_2^* = t\omega_1 + u\omega_2.$$

L'expression

$$d_r = \begin{vmatrix} 1 & \sqrt{m} \\ 1 & -\sqrt{m} \end{vmatrix}^2 = 4m,$$

que l'on peut écrire sous une forme plus générale

$$d_r = \begin{vmatrix} \omega_1 & \omega_2 \\ \omega_1' & \omega_2' \end{vmatrix}^2$$

est le discriminant de l'anneau. On voit qu'il est toujours un multiple du discriminant du corps.

Un *idéal d'anneau* est un système illimité de nombres de l'anneau

$$\mathfrak{j}_r = (\alpha, \beta, \gamma, \ldots \lambda_1\alpha + \lambda_2\beta + \lambda_3\gamma + \ldots),$$

tel que toute combinaison linéaire de nombres quelconques de l'anneau, avec des coefficients $\lambda_1, \lambda_2, \lambda_3, \ldots$, appartenant à l'anneau soit encore un nombre du système.

Il est évident que les notions de *base* d'un idéal de *congruences* suivant un idéal, de *norme* d'un idéal, d'*idéal* conjugué, de *produit* de deux idéaux, s'étendent à l'idéal d'anneau dans le cas particulier que nous avons considéré.

Car, par exemple, soit $\mathfrak{j}_r = (\alpha, \beta, \gamma, \ldots)$ et soit i le plus grand commun diviseur des nombres rationnels de l'anneau. Posons $\alpha = a + b\sqrt{m}$ et désignons par i_2 le plus grand commun diviseur de tous les coefficients b, une base de l'idéal peut toujours être mise sous la forme

$$i,\ i_1 + i_2\sqrt{m} \quad \text{ou} \quad i_1^2 - i_2^2 m \equiv 0\ (i),$$

de plus $n(\mathfrak{j}_r) = ii_2$.

On ne peut cependant pas appliquer ainsi aux idéaux d'anneaux tous les théorèmes vrais pour les idéaux du corps.

Par exemple dans l'anneau $r(\sqrt{-3})$ du corps $k(\sqrt{-3})$, 4 peut être décomposé de deux manières distinctes en facteurs premiers

$$4 = 2.2 = (1 + \sqrt{-3})(1 - \sqrt{-3}),$$

sans que pour cela dans l'anneau un des nombres $1 + \sqrt{3}$ ou $1 - \sqrt{3}$ soit divisible par 2. Il n'y a pas d'identé de la forme

$$1 + \sqrt{-3} = 2.(a + b\sqrt{-3}),$$

où a et b sont des entiers rationnels, ni d'identité de la forme

$$2 = (1 + \sqrt{-3})(a + b\sqrt{-3}).$$

Si l'on voulait obtenir la décomposition unique en facteur, comme on l'a fait dans les exemples antérieurs, c'est-à-dire en employant les idéaux

$$\mathfrak{j} = (2,\ 1 + \sqrt{-3}), \quad \mathfrak{j}' = (2,\ 1 - \sqrt{-3})$$

on n'arriverait plus au résultat. Tandis que dans le corps le produit $\mathfrak{j}\,.\,\mathfrak{j}'$ est un idéal principal, dans l'anneau

$$\mathfrak{j}\,.\,\mathfrak{j}' = (4,\ 2 + 2\sqrt{-3},\ 2,\ -2\sqrt{-3},\ 4\sqrt{-3}, \ldots) = (2)(2,\ 1 + \sqrt{-3})$$

n'est plus un idéal principal.

En fait, l'idéal d'anneau $(2, 1 + \sqrt{-3})$ joue un rôle particulier, il est un idéal principal de $k(\sqrt{-3})$ égal à (2), et on peut en quelque sorte le considérer comme un idéal principal impropre de l'anneau. En tout cas, l'exemple de 4 nous montre que pour les idéaux d'anneau, la décomposition unique en facteurs premiers n'est plus vraie sans restriction.

En général, un idéal du corps n'est pas aussi idéal de l'anneau, mais il y a évidemment une infinité d'idéaux du corps qui sont des idéaux de l'anneau. Le plus grand commun diviseur des idéaux du corps, qui sont aussi des idéaux de l'anneau [dans le cas particulier du corps $k(\sqrt{m})$ l'idéal (2)] est le *conducteur* de l'anneau.

Théorème. — Un idéal du corps $\mathfrak{j}$ est un idéal de l'anneau lorsqu'il est divisible par l'idéal (2), et dans ce cas-là seulement.

Démonstration : Dans le cas où $\mathfrak{j}$ est un idéal du corps divisible par 2, $\mathfrak{j} = (2)\mathfrak{j}$, $\mathfrak{j}$ ne contient que des nombres de l'anneau de la forme $2a$ et $a + b\sqrt{-3}$, $\mathfrak{j}$ est donc un idéal de l'anneau.

Si, de plus, l'idéal du corps $\mathfrak{j} = (a, b + c\sqrt{m})$ est aussi un idéal de l'anneau, a est pair, sans quoi le nombre $a.\omega = a\frac{1+\sqrt{m}}{2}$ contenu dans l'idéal du corps ne le serait pas dans l'anneau, et de même $b - c$ doit être pair, sans quoi $(b - c)\omega' + c\frac{1-m}{2}$ ne serait pas dans l'anneau. Mais a et $b - c$ sont divisibles par 2, $\mathfrak{j}$ l'est par (2).

Il résulte de là que (2) est le conducteur de l'anneau. Introduisons quelques notations dues à M. Hilbert.

Soit $\mathfrak{j}_r = (\alpha, \beta \ldots)$ un idéal d'anneau et $\mathfrak{j} = (\alpha, \beta)$ le plus grand commun diviseur des nombres $\alpha, \beta \ldots$ dans le corps $k(\sqrt{m})$, c'est-à-dire que $\mathfrak{j}$ est un idéal du corps ; nous dirons que $\mathfrak{j}$ est l'*idéal correspondant* à l'idéal $\mathfrak{j}_r$. Lorsqu'en particulier $\mathfrak{j}$ est premier avec le conducteur de l'anneau [(2) dans notre cas particulier], $\mathfrak{j}_r$ est dit *un idéal d'anneau régulier* (1).

---

(1) Pour l'introduction de cette notion nos recherches sont limitées aux idéaux d'anneaux premiers avec f. Ceci est nécessaire. Ex. : lorsque nous avons considéré l'idéal (2) ou $(2, 1 + \sqrt{-3})$, nous avons vu que la décomposition en facteurs des nombres de l'anneau divisibles par 2 nous menait à des contradictions. D'autre part, dans la définition de l'équivalence des idéaux d'anneaux

On montrera tout d'abord, que les lois de divisibilité vraies pour les idéaux du corps s'appliquent aux idéaux d'anneaux réguliers, à condition de définir le produit et le quotient de deux idéaux d'anneaux comme on l'a fait pour les idéaux du corps.

Théorème. — Soit $\mathfrak{j}$ un idéal du corps $k(\sqrt{m})$ premier avec (2), il y a toujours dans l'anneau $r(\sqrt{m})$ un idéal $\mathfrak{j}_r$ auquel correspond l'idéal $\mathfrak{j}$.

Démonstration : Soit

$$\mathfrak{j} = (a, b + c\omega),$$

et soient a et $b + c\omega$ les nombres de base de cet idéal. Si $\mathfrak{j}$ est premier avec (2), a est impair et c l'est aussi. Alors

$$\mathfrak{j}_r = (a, 2b + 2c\omega)$$

est un idéal d'anneau auquel correspond $\mathfrak{j}$. En effet l'idéal correspondant à $\mathfrak{j}_r$ est

$$\mathfrak{j} = (a, 2b + 2c\omega) = (a, b + c\omega),$$

comme

$$-a(b + c\omega) + \frac{a+1}{2}(2b + 2c\omega) = b + c\omega$$

est un nombre du corps qui appartient à l'idéal $\mathfrak{j}$, car $\frac{a+1}{2}$ est un nombre entier rationnel. Comme de plus a est premier avec (2), $\mathfrak{j}_r$ est un idéal d'anneau régulier.

Théorème. — Au produit de deux idéaux d'anneau réguliers,

---

réguliers, on introduit les quotients de nombres entiers. Quoique ces fractions n'aient pas de sens en elles-mêmes, leur emploi est en contradiction avec la définition de l'anneau, qui ne comprend que des entiers. M. Fueter, pour éviter cette difficulté, a introduit cette nouvelle définition de l'anneau d'un corps.

Définition : Tous les nombres (entiers ou fractionnaires) du corps $k(\sqrt{m})$ premiers avec $f = 2$, ou qui sont congrus à 1 suivant f, forment un anneau du corps. (Voir *Journal de Crelles*, t. CXXX, *Le corps quadratique et la multiplication complexe. Diss.*, Göttinger, 1903).

C'est ainsi que l'anneau sert à la généralisation des notions d'idéal et d'équivalence. L'addition n'existe plus. Cette définition convient aux applications de l'arithmétique à l'algèbre supérieure. On voit comment, avec cette nouvelle définition, il faut modifier ce qui précède.

correspond le produit des idéaux du corps correspondant aux facteurs.

Démonstration : Soit

$$\mathfrak{j} = (a,\ b + c\omega), \qquad \mathfrak{h} = (a_1,\ b_1 + c_1\omega)$$

les deux idéaux du corps correspondant à $\mathfrak{j}_r$ et $\mathfrak{h}_r$,

$$\mathfrak{j} \cdot \mathfrak{h} = (aa_1,\ a_1 b + a_1 c\omega,\ ab_1 + ac_1\omega,\ \ldots)$$

correspond à

$$\mathfrak{j}_r\mathfrak{h}_r = (aa_1,\ a_1 2b + a_1 c + a_1 c\sqrt{m},\ a2b_1 + ac_1 + ac_1\sqrt{m},\ \ldots)$$

A l'aide de ces deux théorèmes on peut montrer que tout idéal d'anneau *régulier* ne peut être décomposé que d'une seule façon en un produit d'idéaux d'anneau régulier.

En effet, soit $\mathfrak{j}_r$ un idéal régulier et $\mathfrak{j}$ l'idéal du corps premier avec (2), qui lui est attribué, $\mathfrak{j}$ dans le corps $k(\sqrt{m})$ ne peut être décomposé que d'une seule manière, en un produit d'idéaux premiers, qui sont aussi premiers avec (2). A chacun des facteurs premiers correspond un idéal d'anneau régulier, et l'idéal $\mathfrak{j}$ est celui qui correspond au produit de ces derniers. Mais, par hypothèse, $\mathfrak{j}$ correspond à $\mathfrak{j}_r$. $\mathfrak{j}_r$ est donc lui-même le produit de ces idéaux d'anneaux réguliers.

L'application des faits démontrés pour les idéaux du corps à ceux de l'anneau devient très simple.

Nous indiquerons les propositions suivantes :

La norme d'un idéal d'anneau régulier $n(\mathfrak{j}_r)$ est égale à la norme de l'idéal du corps qui lui correspond, les théorèmes relatifs aux normes subsistent. De plus :

Deux idéaux d'anneaux réguliers $\mathfrak{a}_r$ et $\mathfrak{b}_r$ sont dits équivalents, on écrit $\mathfrak{a}_r \sim \mathfrak{b}_r$ lorsque dans l'anneau il existe deux entiers α et β, tels que $\frac{\mathfrak{a}_r}{\mathfrak{b}_r} = \frac{\alpha}{\beta}$, et si la norme $n\left(\frac{\alpha}{\beta}\right)$ est positive [1].

---

[1] Cette restriction, au sens d'équivalence, évite de grandes complications dans les recherches ultérieures. On peut d'ailleurs apporter cette restriction dans la définition de l'équivalence pour le corps. On aurait pu, par exemple, simplifier le théorème du chap. XXX. (Voir HILBERT, *Zahlb.*, 315 et 316). Le système des caractères de l'idéal $\mathfrak{j}$ est alors toujours le système de t unités

$$\left(\frac{+n(\mathfrak{j}),\ m}{l_1}\right) \cdots \left(\frac{+n(\mathfrak{j}),\ m}{l_t}\right).$$

Tous les idéaux équivalents appartiennent à une classe d'idéaux, on démontre comme avant que le nombre des classes est fini.

Pour les *unités* on a :

Théorème. — Les unités d'un anneau imaginaire $r(\sqrt{m})$ sont ± 1, par contre, dans un anneau réel $r(\sqrt{m})$ il y a une infinité d'unités qui peuvent s'exprimer en fonction de l'une d'entre elles, l'unité fondamentale ε_r sous la forme $\pm \varepsilon_r^e$.

Démonstration : Il suffit de démontrer la proposition pour des corps et des anneaux réels.

Soit $\frac{m-1}{4} \equiv 0\ (2)$, ou encore $m \equiv 1\ (8)$, et soit $\varepsilon = a + b\omega$ l'unité fondamentale du corps $k(\sqrt{m})$, on déduit de

$$n(\varepsilon) = \pm 1 = a^2 + ab + \frac{1-m}{4} b^2,$$

que b est pair et que a est impair. Par suite

$$\varepsilon = a + \frac{b}{2} + \frac{b}{2}\sqrt{m}$$

est une unité de $r(\sqrt{m})$, et l'on peut poser $\varepsilon_r = \varepsilon$.

Si, en second lieu $\frac{m-1}{4}$ est impair, c'est-à-dire $m \equiv 5\ (8)$, et si l'on désigne par $\varepsilon = a + b\omega$ l'unité fondamentale de $n(\varepsilon) = \pm 1$, que ou bien b est pair et a impair, ou bien b est impair et a est pair, ou bien a et b sont impairs. Dans le premier cas on peut encore poser $\varepsilon_r = \varepsilon$; dans les autres cas $\varepsilon^3 = B + C\omega$ est une unité de l'anneau, car

$$C = 3ab(a+b) + b^3\left(1 + \frac{m-1}{4}\right)$$

est pair, et l'on peut prendre $\varepsilon_r = \varepsilon^3$.

La norme de ε_r est positive ou négative suivant que $n(\varepsilon) = \pm 1$.

Ajoutons ici une remarque au sujet de l'hypothèse, que le nombre m de $k(\sqrt{m})$ ne contient pas de facteur au carré.

Abandonnons cette hypothèse et soit $m = f^2 m_1$, il y a deux cas :

1. On peut considérer tous les nombres entiers $\frac{a + b\sqrt{m}}{c}$; car alors

$$\sqrt{m_1} = \frac{\sqrt{m}}{f}, \qquad \frac{1 + \sqrt{m_1}}{2} = \frac{f + \sqrt{m}}{2f}$$

sont aussi des entiers, et le corps $k(\sqrt{m})$, dans toute sa généralité, est identique au corps $k(\sqrt{m_1})$.

2. Si on ne considère que les nombres de la forme $a + b\sqrt{m}$, cela revient à l'étude d'un anneau du corps $k(\sqrt{m_1})$, et cela suppose que l'on a étudié les corps dont le nombre fondamental ne contient point de facteur au carré.

CHAPITRE III

—

APPLICATIONS DE LA THÉORIE DU CORPS QUADRATIQUE

34. Le « dernier théorème » de Fermat. — Fermat a énoncé le théorème suivant :

L'égalité

$$x^n + y^n = z^n$$

n'est pas possible pour $n > 2$, x, y, z étant des entiers rationnels tous différents de o.

(Œuvres de Fermat, t. II, observations sur Diophante, p. 291, II). Fermat ajoute qu'il a démontré ce théorème. Mais dans ses œuvres on trouve une démonstration (Œuvres, t. I, p. 327, XXXIII et p. 340, XLV), en ce qui concerne

$$x^4 + y^4 = z^2$$

on n'en trouve pas d'autre.

Euler (1) est le premier qui parvint à démontrer le théorème pour $n = 3$, plus tard d'autres mathématiciens ont démontré d'autres cas particuliers. Legendre (2) et Lejeune-Dirichlet (3) ont démon-

(1) H. S. Smith. — Collect. papers. Report II, p. 131, donne une notice historique approfondie de la question. M. Hilbert (dans son Zahlber, chap. XXXVI), donne la démonstration de Kummer considérablement simplifiée. L'auteur se rapproche considérablement de cette dernière qui lui semble la meilleure.

(2) Legendre. — *Théorie des nombres*, t. II, p. 1 et 11 ; p. 348 et 352.

(3) Ges. Werke, t. I, p. 1-21. Il s'agit de $n = 5$. Dirichlet indique de plus des classes d'équations impossibles $x^5 + ay^5 = z^5$, etc.

tré l'impossibilité pour $n = 5$, $n = 11$ et $n = 14$, en s'appuyant l'un et l'autre sur des principes différents.

Lamé l'a démontrée pour $n = 7$ (1).

Kummer (2) parvint à démontrer le théorème pour les exposants premiers $n < 100$. Outre les lois de réciprocité, ce sont ces théorèmes qui incitèrent Kummer à ses recherches et à ses découvertes sur les nombres premiers. On ne doute pas que les moyens actuels des mathématiques permettront la solution complète des problèmes.

a) Développements de Fermat.

L'intérêt historique nous engage à exposer d'abord l'idée fondamentale de la démonstration de Fermat et d'Euler.

Nous développons la démonstration de Fermat, de l'impossibilité de

$$x^4 + y^4 = z^2,$$

en suivant l'exposition de Legendre et en faisant les abréviations que nous permet l'étude de la théorie des nombres.

Bien que « $x^4 + y^4 = z^2$ » est impossible, cela signifiera qu'il n'y a pas de valeurs entières non toutes nulles de x, y, z, satisfaisant à cette condition.

On peut admettre que x, y, z n'ont pas de diviseur commun, une division les en débarasserait.

Si

$$x^4 + y^4 = z^2 \tag{1}$$

était possible, il en serait de même de

$$(x^2)^2 + (y^2)^2 = z^2. \tag{1a}$$

D'après cela z ne peut avoir que des facteurs premiers de la forme $4n + 1$, et de plus z étant la somme de deux carrés, toute

---

(1) *Comptes rendus*, 1847. Vol. 24, p. 310.

(2) Plusieurs articles du *Journal de Crelh* : Journal, t. 17, 40. Monattsberichte, du k. Akad. d. Vissensch., Berlin 1847, April Abhandl. du k. Akad. d. Vissensch., Berlin 1857.

solution peut être exprimée en fonction de deux entiers r et s sous la forme

$$x^2 = r^2 - s^2, \quad y^2 = 2rs, \quad z = r^2 + s^2, \tag{3}$$

x, y, z n'ayant pas de facteur commun, r et s ne peuvent en admettre, on peut de plus supposer r et s positifs.

Considérons dès lors

$$x^2 = r^2 - s^2 \quad \text{et} \quad y^2 = 2rs,$$

comme r et s n'ont pas de facteur commun y est pair, et de plus, soit r et $2s$, soit $2r$ et s sont eux-mêmes des carrés.

Soit par exemple

$$r = u^2, \quad 2s = 4v^2,$$

on a

$$x^2 = u^4 - 4v^4, \tag{4}$$

équation satisfaite pour

$$u^2 = a^2 + b^2. \tag{5}$$

$$v^2 = ab, \tag{6}$$

où a et b sont des entiers (positifs) premiers entre eux, de (6) il résulte à nouveau que a et b sont des carrés. Soit donc

$$a = f^2, \quad b = g^2,$$

l'équation (5) nous donne

$$u^2 = f^4 + g^4, \tag{7}$$

cette opération est de la même forme que l'équation primitive, mais

$$\sqrt{r} = u \leqq \frac{y}{\sqrt{2}}, \quad s = \sqrt{2v^2} \leqq \frac{y}{\sqrt{v^2}},$$

car $s \geqq 1$, et

$$r = \frac{y^2}{2s} \leqq \frac{y^2}{2},$$

par suite

$$u \leqq \frac{y}{\sqrt{2}}, \quad v \leqq \frac{y}{\sqrt{2}},$$

de (6) il résulte

$$a = f^2 \leqq \frac{y^2}{4}, \quad b = g^2 \leqq \frac{y^2}{4},$$

$$f \leqq \frac{y}{2}, \quad g \leqq \frac{y}{2}.$$

Soit y le plus petit des deux nombres de (1), nous pouvons dire : Si l'équation (1) admet une solution entière (positive), on peut déduire de cette solution un nouveau système de solutions (positives) plus petites. On peut continuer ainsi indéfiniment.

Mais ceci est contraire au fait qu'il y a qu'un nombre fini d'entiers inférieurs à un entier donné.

L'hypothèse que (1) admet une solution n'est pas admissible.

Nous ajouterons :

1. La démonstration précédente montre que

$$x^4 + y^4 = z^4$$

est impossible, ainsi que

$$x^8 + y^8 = z^2,$$

et que d'une façon générale

$$x^{2^n} + y^{2^n} = z^2.$$

2. Considérons deux des équations (3) de la démonstration précédente, elles ne peuvent être satisfaites par des entiers rationnels x, y, z, r, s. Si donc l'on pose à la place de $x^2 = r^2 - s^2$,

$$r + s = x_1^2, \quad r - s = y_1^2,$$

ce qui est toujours possible, car x^2 doit être impair et $r + s$ et $r - s$ n'ont pas de diviseur commun, il en résulte

$$2r = x_1^2 + y_1^2$$
$$2s = x_1^2 - y_1^2,$$

et par suite

$$2y^2 = 4rs = x_1^4 - y_1^4.$$

Donc l'équation

$$x^4 - y^4 = 2z^2$$

est impossible.

3. L'équation

$$x^4 + y^4 = z^4$$

étant impossible, on ne peut trouver deux nombres r et s, tels que

$$x^2 = r^2 - s^2$$
$$z^2 = r^2 + s^2,$$

l'équation

$$z^2x^2 = r^4 - s^4,$$

que nous écrirons

$$z^2 = x^4 - y^4$$

est impossible.

Fermat a donné de ce dernier résultat l'énoncé suivant : il n'y a pas de triangle rectangle dont les côtés soient mesurés par des entiers, et dont la surface est un carré parfait.

Soient a et b les côtés, c l'hypothénuse, on aurait en nombres entiers

$$xy = f$$
$$x^2 + y^2 = z^2,$$

ou

$$(x - y)^2 = z^2 - 4f^2,$$
$$(x + y)^2 = z^2 + 4f^2$$
$$(x^2 - y^2)^2 = z^4 - (2f)^4$$

qui est impossible.

Pour démontrer le théorème de Fermat nous avons montré que l'existence d'une solution de l'équation (1) entraînerait l'existence d'une infinité d'autres plus petites en valeur absolue. Euler a employé un procédé analogue pour démontrer que

$$x^3 + y^3 = z^3$$

n'admet pas de solution.

Démonstration de M. Sommer.

Si l'équation

$$x^3 + y^3 = z^3$$

est soluble en nombres entiers, on peut toujours admettre que deux des nombres x et y n'ont pas de facteur commun, car un pareil facteur diviserait le troisième et on pourrait débarrasser l'égalité

$$x^3 + y^3 = z^3$$

de ce facteur, par une simple division.

Nous montrerons, tout d'abord, que l'un des trois nombres au moins, x, y ou z, est divisible par 3.

Car si l'on suppose, par exemple, que

$$x \equiv \pm 1 \ (3) \quad \text{et} \quad y \equiv \pm \ (3),$$

il en résulte

$$x^3 \equiv \pm 1 \ (9), \quad y^3 \equiv \pm 1 \ (9),$$

on aurait donc

$$x^3 + y^3 \equiv \left\{ \begin{array}{r} 2 \\ 0 \\ -2 \end{array} \right. (9).$$

Si donc z n'est pas non plus divisible par 3, c'est-à-dire

$$z^3 \equiv \pm 1 \ (9),$$

on a

$$x^3 + y^3 + z^3 \equiv \left\{ \begin{array}{r} \pm 1 \\ \pm 3 \end{array} \right. (9).$$

Mais si

$$x^3 + y^3 - z^3$$

n'est pas divisible par 9 on ne peut avoir

$$x^3 + y^3 - z^3 = 0.$$

Il faut donc que l'un des trois nombres soit divisible par 3.

Des trois nombres x, y, z, un seul peut être pair. On peut donc admettre que deux de ces nombres, x et y par exemple, sont impairs, z alors est nécessairement pair, et l'équation

$$x^3 + y^3 = z^3$$

n'est possible, que si elle est de la forme

$$x^3 + y^3 = 2^{3m}z^3,$$

où m est un entier positif $\geqq 1$.

Nous allons montrer maintenant que z est toujours divisible par 3.

En effet, comme x et y sont impairs, on peut toujours trouver deux entiers premiers entre eux, p et q, tels que

$$x = p + q, \qquad y = p - q,$$

et alors

$$x^3 + y^3 = 2p(p^2 + 3q^2).$$

Le second facteur $p^2 + 3q^2$ est certainement impair, de sorte que l'égalité

$$2p(p^2 + 3q^2) = 2^{3m}z^3$$

n'est possible que si p est pair. Si z n'est pas divisible par 3, p et $p^2 + 3q^2$ n'ont pas de facteur commun, et l'on peut écrire

$$2p = 2^{3m}u^3,$$
$$p^2 + 3q^2 = v^3$$

où u et v sont deux entiers rationnels, dont le produit est égal à z.

Si l'on considère $p^2 + 3q^2$ comme la norme du nombre entier $p + q\sqrt{-3}$ de l'anneau $r(-\sqrt{3})$, $p + q\sqrt{-3}$ est premier avec le conducteur de l'anneau, il faut donc que v se décompose dans cet anneau, c'est-à-dire soit la norme d'un entier, on a donc le droit d'écrire

$$p + q\sqrt{-3} = (f + g\sqrt{-3})^3,$$

ce qui donne

$$p = f^3 - 9fg^2, \qquad q = 3f^2g - 3g^3,$$

q est donc divisible par 3. Si donc l'un des deux nombres

$$x = p + q, \qquad y = p - q,$$

x par exemple, est divisible par 3, p est nécessairement divisible par 3, et par suite y le serait aussi.

Il ne nous reste plus que l'hypothèse $z \equiv 0\ (3)$, c'est-à-dire que l'équation

$$x^3 + y^3 = z^3$$

n'est possible que si elle est de la forme

$$x^3 + y^3 = 2^{3m} \,.\, 3^{3n} \,.\, z^3,$$

où m, n sont des entiers rationnels $\geqq 1$.

Pour résoudre cette dernière équation posons encore

$$x = p + q, \qquad y = p - q,$$
$$x^3 + y^3 = 2q(p^2 + 3q^2) = 2^{3m} \,.\, 3^{3n} \,.\, z^3,$$

et comme

$$2p(p^2 + 3q^2) \equiv 0\ (3^3),$$

et que p et q sont premiers entre eux,

$$p \equiv 0\ (3) \qquad \text{et} \qquad p^2 + 3q^2 \equiv 0\ (3^1).$$

On a alors

$$2p = 2^{3m} 3^{n-1} u^3,$$
$$p^2 + 3q^2 = 3v^3.$$

Le premier membre se décompose dans l'anneau $r(\sqrt{-3})$, et on peut poser

$$p + q\sqrt{3} = \sqrt{-3}\ (f + g\sqrt{-3})^3,$$

où f et g représentent des nombres premiers entre eux, il en résulte

$$p = 9f^2g - 9g^3,$$
$$q = f^3 - 9fg^2,$$

ce qui donne pour

$$2p = 2^{3m} 3^{n-1} u^3$$

l'équation

$$2g(g - f)(g + f) = 2^{3m} 3^{3n-3} u^3.$$

Mais comme g, $g - f$, $g + f$ n'ont pas de facteur commun et que des deux nombres g et f, l'un est pair, l'autre impair, il faut que

$$2g = 2^{3m} 3^{3(n-1)} c^3 \qquad \text{soit} \qquad 2g = 2^{3m} c_1^3$$

ou

$$g - f = b^3 \qquad\qquad g - f = 3^{3(n-1)} b_1^3$$
$$g + f = a^3 \qquad\qquad g + f = a_1^3,$$

mais alors, ou bien

$$a^3 - b^3 = 2^{3m} 3^{3(n-1)} c^3 \qquad \text{soit} \qquad 2^{3m} c_1^3 = 3^{3(n-1)} b_1^3 - a_1^3.$$

Nous avons vu que si l'équation admettait des solutions, le nombre qui est divisible par 3 le serait aussi par 2, la première de ces deux dernières équations seule serait possible, et par suite des solutions de l'équation donnée, on pourrait déduire une solution de

$$x^3 + y^3 = 3^{3(n-1)} z^3,$$

et en répétant ce raisonnement on arriverait à résoudre

$$x_1^3 + y_1^3 = z_1^3,$$

où aucun des nombres x_1, y_1, z_1 n'est divisible par 3, ce qui est impossible. L'équation

$$x^3 + y^3 = z^3$$

n'a donc pas de solution.

Etudions maintenant ces théorèmes d'après la théorie des corps de nombres.

c Méthodes de Kummer et de Hilbert.

Kummer a généralisé le théorème de Fermat, il a montré que l'équation

$$x^n + y^n + = z^n$$

n'admet pas de solution dans les corps déterminés par $\sqrt[n]{1}$.

Pour le cas de $n = 3$, le théorème de Kummer s'énonce :

Théorème. — L'équation

$$\alpha^3 - \beta^3 = \gamma^3$$

n'admet pas de solution en nombres entiers du corps $k(\sqrt{-3}$, ou encore α, β, γ étant trois entiers différents de o du corps $k(\sqrt{-3})$, il ne peut y avoir entre eux aucune relation de la forme

(1) $$\alpha^3 - \beta^3 = \gamma^3.$$

Démonstration : Le nombre des classes des corps $k(\sqrt{-3})$ $h = 1$, posons ici $\omega = \frac{-1 + \sqrt{-3}}{2}$. Si (1) admet une solution α, β, γ, deux quelconques des nombres α, β, γ sont premiers entre eux. Soit

$$\lambda = 1 - \omega,$$

c'est-à-dire

$$(\lambda) = (\sqrt{-3}),$$

l'un des trois nombres α, β, γ est divisible par λ.

Car si α et β ne sont pas divisibles par λ, et si l'on pose

$$\alpha = a + b\omega = (a + b) - b(1 - \omega),$$

$a + b$ n'est pas divisible par λ, et par suite il ne l'est pas par 3, et comme

$$a + b \equiv \pm 1 \ (3),$$

il en résulte

$$\alpha \equiv \pm 1, \ (\lambda),$$
$$\beta \equiv \pm 1, \ (\lambda),$$

on a donc

$$\alpha^3 + \beta^3 \equiv \begin{cases} -2 \\ 0 \\ 2 \end{cases} (\lambda^3).$$

Si donc γ est premier avec λ

$$\gamma \equiv \pm 1 \ (\lambda),$$

et alors

$$\alpha^3 + \beta^3 + \gamma^3 \equiv \begin{cases} \pm 3 \\ \pm 1 \end{cases} (\lambda^3),$$

ce qui est contraire à l'hypothèse, car

$$\pm 3 \not\equiv 0, \qquad \pm 1 \not\equiv 0 \ (\lambda^3).$$

Soit donc

$$\gamma = \lambda^n \gamma_1, \qquad n \geqq 1,$$

on voit de plus qu'il faut $n \geqq 2$.

Considérons le nombre $\alpha = a + b\omega$ premier avec λ, on a ou bien

$$a \equiv \pm 1 \ (3), \qquad b \equiv 0 \ (3),$$

et l'on peut poser

$$\alpha = \pm 1 + \lambda^2\alpha_1,$$

α_1 étant un entier du corps, ou bien

$$a \equiv \pm 1 \ (3) \quad \text{avec} \quad b \equiv \pm 1 \ (3),$$

parce qu'on a

$$a + b \equiv \pm 1 \ (3),$$

alors on a

$$\alpha = a + b\omega = \pm(1 + \omega) + \lambda^2\alpha_1,$$

où

$$\eta = 1 + \omega$$

est une unité du corps.

On a donc

$$\alpha \equiv \eta \ (\lambda^2),$$

et de même

$$\beta \equiv \eta_1 \ (\lambda^2),$$

η_1 étant aussi une unité du corps. Mais comme

$$\alpha^3 - \beta^3 \equiv 0 \ (\lambda^3),$$

il faut que

$$\eta^3 - \eta_1^3 = 0,$$

et par suite

$$\alpha^3 - \beta^3 \equiv 0 \ (\lambda^4).$$

γ est donc divisible par λ^2 au moins.

Nous allons démontrer que l'égalité un peu plus générale que la proposée

(2) $$\alpha^3 - \beta^3 = \eta\lambda^{3m}\gamma_1^3,$$

où η est une unité du corps, est impossible.

Par suite de

$$\alpha \equiv \pm 1, (\lambda), \qquad \beta \equiv \pm 1, (\lambda),$$
$$\alpha^3 - \beta^3 \equiv 0 \ (\lambda^3),$$

il faut que α et β satisfassent à la fois à

$$\alpha \equiv +1, (\lambda), \qquad \beta \equiv +1 \ (\lambda)$$
$$\alpha \equiv -1, (\lambda), \qquad \beta \equiv (-1) \ (\lambda),$$

d'où l'on a les congruences simultanées

$$\left.\begin{array}{r} \alpha - \beta \equiv 0 \\ \alpha - \omega\beta \equiv 0 \\ \alpha - \omega^2\beta \equiv 0 \end{array}\right\} (\lambda).$$

Une seule, des trois différences $\alpha - \beta$, $\alpha - \omega\beta$, $\alpha - \omega^2\beta$, peut contenir λ à une puissance supérieure à 1, car si l'on admet que $\alpha - \beta$ est divisible au moins par λ^2, $\alpha - \omega\beta$ et $\alpha - \omega^2\beta$ ne peuvent être divisibles que par λ, car on a par exemple

$$\frac{\alpha - \omega\beta}{\lambda} \equiv \pm 1 \ (\lambda),$$

comme de plus α et β sont premiers entre eux, les trois nombres $\alpha - \beta$, $\alpha - \omega\beta$, $\alpha - \omega^2\beta$ ne peuvent avoir d'autre facteur commun que λ, de sorte que l'équation (2), ou encore l'équation

$$(2_a) \qquad (\alpha - \beta)(\alpha - \omega\beta)(\alpha - \omega^2\beta) = \eta\lambda^{3n}\gamma^3$$

ne peut être satisfaite qu'en posant :

$$(3) \qquad \left\{\begin{array}{l} \alpha - \beta = \eta_1\lambda^{3n-2}\tau^3 \\ \alpha - \omega\beta = \eta_2\lambda\mu^3 \\ \alpha - \omega^2\beta = \eta_3\lambda\nu^3, \end{array}\right.$$

où η_1, η_2, η_3 sont des unités du corps, et où τ, μ, ν sont des entiers sans facteur commun, mais on sait que :

$$\omega(\alpha - \beta) + \omega^2(\alpha - \omega\beta) + (\alpha - \omega^2\beta) = 0,$$

il résulte de (3) que

$$\omega\eta_1\lambda^{3n-2}\tau^3 + \eta_2\omega^2\lambda\mu^3 + \eta_3\lambda\nu^3 = 0,$$

c'est-à-dire en divisant par $\omega^2\varkappa_2\lambda$ et en désignant par ζ_1 et ζ les unités qui restent

$$\mu^3 - \zeta\nu^3 = \zeta_1\lambda^{3(n-1)}\xi^3,$$

comme $n \geqq 2$, on peut considérer cette équation comme une congruence suivant le module λ^2, qu'on écrit

$$\mu^3 - \zeta\nu^3 \equiv 0\ (\lambda^2).$$

Mais on a $\mu, \nu \equiv \pm 1\ (\lambda)$ et $\mu^3, \nu^3 \equiv \pm 1\ (\lambda^2)$, la dernière équation nous apprend donc que

$$\zeta \equiv \pm 1\ (\lambda^2),$$

c'est-à-dire

$$\zeta = \pm 1.$$

Si donc l'équation (2) admet des solutions, on voit que

$$\alpha^3 - \beta^3 = \zeta_1\lambda^{3(n-1)}\xi^3$$

en admet aussi.

En répétant ce raisonnement on arrive à l'équation

$$\alpha^3 - \beta^3 = \eta_1\lambda^3\gamma^3,$$

où les trois nombres α, β, γ ne contiennent plus le facteur λ, et nous avons vu que dans ces conditions l'équation est impossible. Il est donc impossible de satisfaire à (2) au moyen de nombres du corps $k(\sqrt{-3})$.

Pour terminer nous indiquerons encore la généralisation de Kummer, du théorème de Fermat, pour $n = 4$.

Théorème. — L'équation indéterminée

$$\alpha^4 + \beta^4 = \gamma^2$$

ne peut être satisfaite par trois nombres du corps $k(\sqrt{-1})$, tous différents de zéro.

Admettons qu'on ait

$$(1) \qquad \alpha^4 = \gamma^2 - \beta^4,$$

où α, β, γ n'ont pas de facteur commun.

Soit

$$\lambda = 1 - \sqrt{-1}.$$

l'un des trois nombres admettra le facteur λ, tandis que les autres ne l'admettront pas.

2 et $\pm(1 \pm \sqrt{-1})$ sont divisibles par λ, car $n(\lambda) = 2$ et $\lambda' = \sqrt{-1}\,\lambda$. Tout nombre entier du corps premier avec λ satisfait à

$$\alpha \equiv \sqrt{-1}\ (\lambda),$$

de plus, tout nombre entier du corps premier avec 2, satisfait à l'une des congruences

$$(2) \qquad \alpha \equiv \sqrt{-1}\ (2) \qquad \text{ou à} \qquad \alpha \equiv 1\ (2),$$

car il n'y a que deux restes premiers avec 2.

Chacune de ces deux congruences (2) nous montre que

$$\alpha^4 - 1 \equiv 0\ (\lambda^6),$$

c'est-à-dire que tout nombre entier du corps voit sa quatrième puissance congrue à $+1$, suivant le module 8.

Supposons d'abord α, β de l'égalité (1) premiers avec λ. On a

$$(3) \qquad \alpha^4 \equiv 1\ (\lambda^6), \qquad \beta^4 \equiv 1\ (\lambda^6),$$

$$\alpha^4 + \beta^4 - 2 \equiv 0\ (\lambda^6),$$

$$(4) \qquad \alpha^4 + \beta^4 - 2 = \gamma^2 - 2,$$

il en résulte que $\gamma = \lambda\gamma_1$, γ_1 étant premier avec λ, c'est-à-dire que

$$\gamma^2 - 2 = \lambda^2\gamma_1^2 - 2 = -2\sqrt{-1}\,(\gamma_1^2 - \sqrt{-1}),$$

c'est-à-dire

$$\gamma_1^2 - \sqrt{-1} \equiv 0\ (\lambda^4),$$

ceci n'est pas possible, car pour un entier γ_1 on ne peut avoir que

$$\gamma_1^2 \equiv +1, \qquad \gamma_1^2 \equiv -1\ (\lambda^4).$$

Si l'on admet en second lieu que β et γ sont premiers avec λ, on a toujours

$$\gamma^2 \equiv 1\ (\lambda^2) \qquad \text{et} \qquad \beta^4 \equiv 1\ (\lambda^2),$$

$\gamma^2 - \beta^4$ est divisible au moins par λ^2 ; c'est-à-dire que

$$\alpha \equiv 0\ (\lambda) \qquad \text{ou} \qquad \alpha = \lambda^n\alpha_1\ (n \geqq 1).$$

L'équation (1) n'est donc possible que s'il en est ainsi de

$$\lambda^{4n}\alpha^4 = \gamma^2 - \beta^4,$$

et réciproquement.

Nous remplacerons cette dernière par une équation un peu plus générale

$$(5) \qquad \varepsilon\lambda^{4n}\alpha^4 = \gamma^2 - \beta^4,$$

où ε est une unité du corps $k(\sqrt{-1})$.

On peut mettre (5) sous la forme

$$\gamma^2 - 1 = \varepsilon\lambda^{4n}\alpha^4 + \beta^4 - 1,$$

et comme

$$\beta^4 - 1 \equiv 0\ (\lambda^6),$$

on en conclut que $\gamma^2 - 1$ est divisible au moins par λ^4, ceci n'est possible que si $\gamma \equiv 1\ (\lambda^2)$, posons

$$\gamma - 1 = \lambda^2\tau,$$

on a

$$\gamma + 1 = \lambda^2(\tau + \sqrt{-1}),$$

et comme $\tau + \sqrt{-1}$ est divisible par λ, on a

$$\gamma^2 - 1 \equiv 0\ (\lambda^5),$$

le second membre de (5) est donc divisible par λ^5, ceci exige que $n \leqq 2$.

Nous écrirons (5)

$$(6) \qquad \varepsilon\lambda^{4n}\alpha^4 = (\gamma - \beta^2)(\gamma + \beta^2),$$

et nous remarquerons que $\gamma - \beta^2$, $\gamma + \beta^2$ ne peuvent avoir d'autre diviseur commun que λ^2, on peut remplacer (6) par

$$(7) \qquad \begin{cases} \gamma - \beta^2 = \eta\lambda^2\sigma^4 \\ \gamma + \beta^2 = \eta_1\lambda^{4n-2}\tau^4, \end{cases}$$

où σ et τ sont deux entiers premiers entre eux et où η et η_1 sont des unités. On tire de là

$$(8) \qquad 2\beta^2 = \eta_1\lambda^{4n-2}\tau^4 - \eta\lambda^2\sigma^4.$$

ou en divisant par 2 et en remplaçant $-\frac{\tau_1\lambda^2}{2}$, $\frac{\tau_1\lambda^2}{2}$ par ζ, ζ_1. Ces dernières lettres désignant des unités, on a

$$(9) \qquad \beta^2 - \zeta\sigma^4 = \zeta_1\lambda^{4(n-1)}\tau^4.$$

Comme $n \geqq 2$, on voit que

$$\beta^2 - \zeta\sigma^4 \equiv 0\ (\lambda^4) \qquad \text{ou} \qquad \beta^2 - \zeta \equiv 0\ (\lambda^4),$$

il en résulte que $\zeta = \pm 1$. C'est-à-dire que lorsque l'équation (5) admet des solutions, il en est de même de

$$(10) \qquad \varepsilon\lambda^{4(n-1)}\alpha^4 = \gamma^2 - \beta^4.$$

En répétant ce raisonnement on arriverait à cette conclusion

$$\varepsilon\lambda^4\alpha^4 = \gamma^2 - \beta^4$$

admet des solutions, ce qui contredit la condition trouvée, que n doit être $\geqq 2$.

Le théorème est donc démontré.

Cette démonstration nous permet d'affirmer que

$$z^2 = x^4 + y^4$$
$$z^2 = x^4 - y^4$$

n'admettent pas de solution entière rationnelle où x, y, z sont tous différents de zéro.

On peut aussi dire que les équations

$$x^3 + y^3 = z^3$$
$$x^4 \pm y^4 = z^2$$

ne peuvent être vérifiées par trois nombres rationnels entiers ou fractionnaires, tous trois différents de zéro.

Comme conséquence immédiate, les équations

$$x^{3n} + y^{3n} = z^{3n}$$
$$x^{4n} \pm y^{4n} = z^{2n} \qquad n > 1$$

ne sont pas possibles en nombres entiers, dont aucun n'est nul.

Le théorème de Fermat peut s'énoncer autrement : quel que soit le nombre rationnel x les nombres

$$\sqrt[3]{1 \pm x^3}, \qquad \sqrt{1 \pm x^4}$$

sont irrationnels.

On peut encore dire : les courbes

$$x^3 \pm y^3 = c^3$$
$$x^4 \pm y^4 = c^2,$$

où c est rationnel, ne passent par aucun point dont les coordonnées sont rationnelles.

L'équation

$$x^3 \pm y^3 = z^3$$

ne peut être satisfaite par des racines carrés de nombres rationnels non carrés, dont aucune n'est nulle.

On ne peut avoir

$$\sqrt{a^3} \pm \sqrt{b^3} = \sqrt{c^3},$$

sans quoi on aurait

$$a^3 + b^3 - c^3 = \mp 2\sqrt{a^3b^3},$$

ce qui n'est pas possible, car a, b ne sont pas carrés parfaits et n'ont pas de facteur commun.

Kronecker [1] a tiré une conséquence importante dans l'étude du corps algébrique du 3e degré, de ce fait que

$$x^3 + y^3 = 1$$

n'admet d'autre solution rationnelle que $x = 0$, $y = 1$ ou $x = 1$, $y = 0$.

Si cette équation admet une solution rationnelle, on pourrait mettre x et y sous la forme

$$x = \frac{2a}{3b - 1}, \qquad y = \frac{3b + 1}{3b - 1},$$

---

[1] Kronecker, *Œuvres*, t. I, 1895, p. 121, ou *Journal de Crelle*, t. LVI, p. 188.

et alors

$$x^3 + y^3 - 1 = \frac{2(4a^3 + 27b^2 + 1)}{(3b-1)^3},$$

et toute solution rationnelle x et y nous donnerait une solution rationnelle de

$$4a^3 + 27b^2 + 1 = 0.$$

Mais comme la première n'admet que $x = 1$, $y = 0$, ou $x = 0$, $y = 1$), l'équation

$$4a^3 + 27b^2 + 1 = 0$$

ne peut admettre que les solutions

$$a = -1, \; b = \pm \frac{1}{3}.$$

Si maintenant l'on remarque que

$$\Delta = -(4a^3 + 27b^2)$$

est le discriminant de l'équation

$$x^3 + ax + b = 0,$$

il en résulte :

Théorème. — Les équations

$$x^3 - x \pm \frac{1}{3} = 0$$

sont les seules équations du troisième degré dont la somme des racines est nulle et dont le discriminant $= +1$.

Nous n'examinerons pas ici les cas de $x^n + y^n = z^n$ où $n \geqq 5$. Nous allons appliquer la théorie du corps quadratique à l'étude des propriétés des formes quadratiques.

35. Un aperçu des problèmes fondamentaux de la théorie des formes quadratiques. — Lorsque nous avons étudié certains corps particuliers comme $k(\sqrt{-1})$, $k(\sqrt{2})$, etc., nous avons obtenu les conditions pour qu'un nombre rationnel a puisse être mis sous la forme

$$x^2 + y^2 \quad \text{ou} \quad x^2 - 2y^2 \quad \text{ou} \quad x^2 + 3y^2,$$

ou encore, les conditions pour qu'une équation de la forme

$$a = x^2 - my^2$$

admette des solutions en nombres entiers x et y.

Ce sont des cas particuliers d'une théorie générale, la théorie des formes quadratiques.

Toute expression de la forme

$$f = ax^2 + 2bxy + cy^2,$$

où a, b, c sont des nombres donnés, et x, y des variables, est dite une *forme quadratique*, et nous admettrons toujours que a, $2b$, c sont des *entiers* rationnels. a, b, c sont appelés les coefficients de la forme, a, c les coefficients extrêmes, b le coefficient moyen.

Dans ses recherches, Gauss a toujours pris $2b$ pair.

Euler avait déjà trouvé des résultats remarquables en étudiant certaines formes particulières, mais Lagrange est le premier qui aborda l'étude de la forme quadratique la plus générale, il en découvrit les propriétés au moyen des fractions continues. Legendre a exposé ses recherches dans sa *Théorie des nombres*.

Gauss [1] fit faire le plus grand progrès à la théorie des formes quadratiques. Presque toute la *sectio V des Disquis. arith.* lui est consacrée.

La méthode de Gauss est demeurée un modèle dans la théorie des nombres, c'est Gauss aussi qui a signalé les problèmes les plus féconds et les plus profonds.

Nous allons expliquer une série de notations indispensables, nous indiquerons les questions fondamentales de la théorie, et enfin nous montrerons ses rapports avec la théorie du corps quadratique.

Gauss dit que la forme quadratipue

$$F = ax^2 + 2bxy + cy^2$$

est proprement primitive, lorsque a, $2b$, c n'ont pas de facteur

---

[1] Le lecteur est prié de lire, outre les œuvres citées de Gauss et de Legendre, les chapitres de Dirichlet-Dedekind et de Bachmann, etc.

commun, et improprement primitive lorsqu'ils admettent le facteur premier commun 2. Le discriminant

$$D = b^2 - ac$$

est dit le *déterminant* de la forme. Ce déterminant peut être positif ou négatif et son signe joue un rôle important, c'est d'ailleurs aussi ce qui se présente pour les corps réels et les corps imaginaires.

Nous ne traiterons que le cas le plus important, celui où D n'a pas de facteur carré. Nous excepterons toujours $D = 0$.

Lorsque, dans une forme F de déterminant D, on remplace x, y par de nouvelles variables x_1, y_1, à l'aide d'une substitution à coefficients entiers rationnels, on obtient une nouvelle forme

$$f = Ax_1^2 + 2Bx_1y_1 + Cy_1^2.$$

Le déterminant de la forme f qui est dite obtenue par transformation de F est

$$D_1 = \begin{vmatrix} r & s \\ t & u \end{vmatrix}^2 D = \Delta^2 D,$$

où Δ est le déterminant de la transformation.

Lorsque $\Delta \neq \pm 1$ on dit que la forme f est contenue dans F, par contre si $\Delta = \pm 1$ on dit que les formes F et f sont équivalentes, si $\Delta = +1$ proprement équivalentes, et improprement équivalentes si $\Delta = -1$. Dans ces deux derniers cas, comme on le voit, la forme f est contenue dans F et réciproquement F est contenue dans f.

En prenant $ru - st = +1$, on peut déduire d'une forme une infinité d'autres formes, qui lui sont proprement équivalentes. Deux transformations successives équivalent à une seule dont le déterminant est le produit des deux premiers ; par suite, deux formes équivalentes à une troisième sont équivalentes entre elles. On obtient donc toutes les formes équivalentes, en partant de l'une d'entre elles. On dit que toutes les formes équivalentes entre elles forment une *classe*.

On démontre que toutes les formes de déterminant donné D peuvent être réparties en un nombre *fini* de classes.

Les problèmes fondamentaux de la théorie des formes quadratiques sont les suivants :

1. Savoir si un nombre donné est représentable par une forme donnée, et connaître les valeurs de x et y qui permettent cette représentation.

2. Reconnaître si deux formes quadratiques données, de même déterminant D, sont équivalentes, et trouver les formules de transformation qui font passer de l'une à l'autre.

3. Démontrer que les formes en nombre illimité forment un nombre fini de classes.

4. Trouver des formes représentant chaque classe afin de simplifier les calculs du premier problème.

C'est précisément ce premier problème qui a donné l'occasion de toutes les recherches sur les formes quadratiques, c'est en quelque sorte *le problème* des formes quadratiques.

Lorsqu'un nombre est représentable par une forme quadratique F, il l'est par toute forme F_1 équivalente à F. On simplifiera donc la solution du premier problème, on cherchera donc des formes simples pouvant donner le plus facilement la représentation d'un nombre donné.

Un autre problème de la théorie consiste à répartir les classes en genres.

En 1801, au temps où Gausse publiait ses recherches sur l'arithmétique supérieure, les nombres imaginaires n'avaient pas les mêmes droits que les nombres réels. On les négligeait parce qu'on croyait y voir des contradictions, et parce qu'ils avaient été l'objet de mainte application erronée.

Gauss, quoique ne partageant pas ce préjugé, n'employa cependant pas les imaginaires, et il bâtit sa théorie des formes quadratiques en se fondant sur les propriétés des nombres réels.

Kummer [1] dès ses premières communications au sujet de la découverte des idéaux, a montré que la théorie des formes quadratiques et que la théorie des corps quadratiques étaient identiques.

L'emploi des nombres quadratiques permet de simplifier beaucoup la théorie des formes (Voir Dedekind, *Vorlesungen über Zahlentheorie von Lejeune-Dirichlet*, § 71 et suppl. XI, § 186).

Nous allons examiner ici de plus près le rapport entre les formes

---

(1) *Journal de Crelle*, t. XXXV, p. 325.

et les corps. Il faut établir pour cela une correspondance exacte entre un idéal et une forme quadratique, l'application de la multiplication des idéaux des idées de classe et de genre se fera d'elle-même.

La correspondance entre les idéaux et les formes est un peu plus compliquée pour les corps réels que pour les corps imaginaires. Nous traiterons donc principalement le cas des corps réels.

36. La correspondance des idéaux et des formes quadratiques. — (*La représentation des nombres par des formes quadratiques*). Soit $\mathfrak{p} = (p, b + \sqrt{m})$ un idéal premier du corps $k(\sqrt{m})$, alors tous les nombres de l'idéal peuvent être représentés par $px + (b + \sqrt{m})y$, où x et y prennent toutes les valeurs entières rationnelles. Les normes

$$p(px^2 + 2bxy + \frac{b^2 - m}{p}y^2)$$

contiennent toutes une forme de déterminant m en facteur. On est donc amené à attribuer la forme

$$px^2 + 2bxy + \frac{b^2 - m}{p}y^2$$

à l'idéal $\mathfrak{p}$, ou aux normes en nombre infini des nombres de l'idéal. Examinons les différents cas :

1er *Cas*. — *Le corps est réel* $k(\sqrt{m})$

$$m \equiv 2 \quad \text{ou} \quad m \equiv 3 \ (4),$$

c'est-à-dire soit $k(\sqrt{m})$ un corps de déterminant $d = 4m$, de base 1, $\omega = \sqrt{m}$ et ayant un nombre quelconque de classes h. Soit p un nombre premier rationnel, il y a trois cas possibles.

*) Ou bien $\left(\frac{d}{p}\right) = -1$, (p) est premier dans $k(\sqrt{m})$, cela veut dire que p ne peut être représenté par aucun nombre de la forme $x^2 - my^2$, il en résulte de plus que p ne peut être représenté par aucune forme $ax^2 + 2bxy + cy^2$ de déterminant $b^2 - ac = m$. En effet, comme $\left(\frac{d}{p}\right) = \left(\frac{m}{p}\right) = -1$, les coefficients extrêmes sont premiers avec p ; dans le cas où $\pm p = ax^2 + 2bxy + cy^2$ aurait des solutions, $\pm ap = (ax + by)^2 - my^2$ en aurait aussi, ce qui est contraire à l'hypothèse $\left(\frac{m}{p}\right) = -1$.

**) Ou bien $\left(\frac{d}{p}\right) = +1$, (p) se décompose dans le corps $k(\sqrt{m})$ en un produit de deux idéaux principaux ou de deux idéaux non principaux.

***) Ou bien $\left(\frac{d}{p}\right) = 0$, alors (p) est le carré d'un idéal premier ambige.

Idéaux principaux et formes principales.

Supposons que (p) égale le produit de deux idéaux principaux

(1) $$(p) = (a + b\omega)(a + b\omega'),$$

cela veut dire que p peut être représenté par l'une des deux formes,

(I) $$f = x^2 - my^2,$$
(II) $$f = -x^2 + my^2,$$

ou bien encore par toutes les deux.

Si la norme de l'unité fondamentale ε du corps $k(\sqrt{m})$ est égale à $+1$, l'égalité (1) montre que l'une seule des deux égalités suivantes est possible

$$p = a^2 - mb^2 \quad \text{ou} \quad -p = a^2 - mb^2,$$

par contre, si $\varepsilon = r + s\sqrt{m}$ et que $n(\varepsilon) = -1$, et si l'on a

$$p = a^2 - mb^2,$$

on a aussi

$$-p = (a^2 - mb^2)(r^2 - ms^2),$$

mais le second membre peut être considéré comme la norme d'un nombre entier

$$ar + bm + (as + br)\sqrt{m},$$
$$-p = (ar + bsm)^2 - m(as + br)^2,$$

p et $-p$ sont représentables par les mêmes formes quadratiques I et II.

Supposons qu'on ait $+p = a^2 - mb^2$ et faisons d'abord $x = a$, $y = b$, puis $x = ar + bsm$, $y = as + br$, dans I nous aurons $+p$ et $-p$. Faisons les mêmes substitutions dans II, nous aurons $-p$ et $+p$.

D'autre part, comme

$$n(\varepsilon) = r^2 - ms^2 = -1,$$

la forme II devient la forme I par la transformation

$$(3) \qquad \begin{cases} x_1 = rx + msy \\ y_1 = -sx - ry, \end{cases}$$

dont le déterminant est $+1$.

Réciproquement, s'il existe une transformation de déterminant $+1$ qui fait passer de I à II, p et $-p$ peuvent être représentés à la fois par $x^2 - my^2$ et $-x^2 + my^2$.

Si

$$+p = a^2 - mb^2, \qquad -p = a_1^2 - mb_1^2,$$

on a nécessairement des égalités de la forme

$$a + \sqrt{m}b = a_1 + \sqrt{m}b_1,$$

et de là il résulte que $\varepsilon = \dfrac{a + \sqrt{m}b}{a_1 + \sqrt{m}b_1}$ est une unité du corps pour laquelle $n(\varepsilon) = -1$.

Les formes I et II sont des formes ayant le déterminant m, nous avons donc le droit de faire la convention suivante.

Soit $\mathfrak{p} = (a - b\sqrt{m})$ ou $\mathfrak{p}' = (a - b\sqrt{m})$ est un idéal principal premier du corps $k(\sqrt{m})$, et soit ε l'unité fondamentale du corps, nous attribuerons aux idéaux $\mathfrak{p}$, $\mathfrak{p}'$:

A. La forme proprement primitive $x^2 - my^2$, lorsque $n(\varepsilon) = -1$;

B. Les deux formes proprement primitives, non équivalentes, $x^2 - my^2$ et $-x^2 + my^2$, lorsque $n(\varepsilon) = +1$.

Posons dans les formules I ou II

$$\begin{aligned} x &= rx_1 + sy_1 \\ y &= tx_1 + uy_1, \end{aligned}$$

et prenons r, s, t, u, tels que $ru - st = +1$, les deux formes quadratiques nous donneront deux systèmes illimités de formes quadratiques

$$(\mathrm{I}_a) \qquad (r^2 - mt^2)x_1^2 + 2(rs - mtu)x_1y_1 + (s^2 - mu^2)y_1^2$$

et

$$(\mathrm{II}_a) \qquad -(r^2 - mt^2)x_1^2 - 2(rs - mtu)x_1y_1 - (s^2 - mu^2)y_1^2,$$

que nous écrirons sous forme abrégée

$$(\mathrm{I}_a) \qquad Ax^2 + 2Bxy - Cy^2,$$

$$(\mathrm{II}_a) \qquad -Ax^2 - 2Bxy + Cy^2.$$

Le déterminant de ces formes est

$$D = B^2 - AC = m.$$

Si le nombre premier p qui peut être représenté par l'une des formes I ou II peut être représenté aussi par l'une des formes I_a et II_a, et réciproquement.

Dans le cas $n(\varepsilon) = +1$ les deux systèmes de formes I_a et II_a sont différents, dans le cas $n(\varepsilon) = -1$ les formes I_a et II_a sont équivalentes, car I et II le sont aussi.

Ce qui est surtout important, c'est la réciproque que nous énoncerons à nouveau.

Tout nombre premier p qui peut être représenté par la forme quadratique

$$F = Ax^2 + 2Bxy + Cy^2$$

de déterminant $D = m$, cette forme est équivalente à l'une des formes I ou II.

On a supposé que $D = B^2 - AC$ ne peut renfermer aucun facteur au carré, les trois coefficients A, B, C ne peuvent avoir aucun facteur commun. On peut admettre de plus, que l'un des trois coefficients A, B, C, par exemple A, est premier avec un nombre donné, en particulier avec le nombre premier p. Cette hypothèse ne restreint pas la généralité ; car si A n'est pas premier avec p, on peut déduire de F une forme équivalente, dont le premier coefficient est premier avec A. Car si A est divisible par p, sans que C le soit (ce qui arrive nécessairement pour $p = 2$), il suffit de faire une transformation unité

$$x = px_1 + sy_1, \qquad y = qx_1 + uy_1,$$

où q est premier avec p. Si C était divisible par p on choisirait une transformation unité

$$x = q_1x_1 + sy_1, \qquad y = q_2x_2 + uy_1,$$

où q_1 et q_2 seraient premiers avec p.

Soient x_1, y_1 deux entiers rationnels premiers entre eux, tels que

(4) $$p = Ax_1^2 + 2Bx_1y_1 + Cy_1^2,$$

on a

(5) $$Ap = (Ax_1 + By_1)^2 - my_1^2,$$

c'est-à-dire que Ap peut être représenté par la forme $x^2 - my^2$. L'équation (4) nous montre que y_1 est premier avec p, et que A et y_1 sont premiers entre eux, et (5) exige que $Ax_1 + By_1$ et y_1 soient premiers avec Ap. Si donc on a

$$p = x^{*2} - my^{*2},$$

où x^* et y^* sont premiers entre eux, on a l'égalité idéale

$$(Ax_1 + By_1 + \sqrt{m}y_1)(Ax_1 + By_1 - \sqrt{m}y_1)$$
$$= (A)(x^* + \sqrt{m}y^*)(x^* - \sqrt{m}y^*),$$

il en résulte que (A) est le produit de deux idéaux principaux, ou que $+$ A est représentable par la forme I. En effet, il faut que $(x^* + \sqrt{m}y^*)$, qui est un idéal premier, soit contenu dans l'un des facteurs du premier membre, de même $x^* - \sqrt{m}y^*$.

Les nombres $Ax_1 + By_1$, y_1, x^*, y^* étant premiers, les uns avec Ap, les autres avec p, il en résulte que l'égalité

$$A = x^2 - my^2$$

est toujours satisfaite par des nombres premiers entre eux et premiers avec A,

$$x = r, \qquad y = t.$$

Soient donc r et t deux entiers rationnels premiers entre eux, tels que

(6) $$+ A = r^2 - mt^2,$$

déterminons deux nombres rationnels s, u, satisfaisant à

$$(7) \qquad ru - ts = 1$$

$$(8) \qquad -tmu + rs = B,$$

c'est-à-dire

$$(9) \qquad u = \frac{Bt + r}{A}, \qquad s = \frac{Br + tm}{A},$$

le nombre

$$(10) \qquad s^2 - mu^2 = \frac{1}{A^2}(B^2 - m)(r^2 - mt^2) = C$$

est un entier rationnel.

On a

$$Ap = (r^2 - mt^2)(x^{*2} - my^{*2}),$$

ou encore

$$(11) \quad Ap = [rx^* + tmy^* + (ry^* + tx^*)\sqrt{m}][rx^* + tmy^* - (ry^* + tx^*)\sqrt{m}].$$

Comparant (11) et (5) on voit que l'on peut choisir x_1 et y_1, tels que

$$Ax_1 + By_1 = rx^* + tmy^*, \qquad -y_1 = tx^* + ry^*,$$

ce qui nous donne

$$(12) \qquad x^* = rx_1 + sy_1, \qquad y^* = -tx_1 - uy_1.$$

D'après ce que nous avons dit x_1, y_1, x^*, y^*, r et t sont des nombres entiers, sy_1 et uy_1 sont des entiers : s et u ne peuvent avoir en dénominateur que des facteurs de y_1, ou, en tenant compte de (9), les nombres rationnels s et u ne peuvent avoir comme dénominateur que des diviseurs communs à A et à y_1. Mais ces deux nombres A et y_1 sont premiers entre eux, s et u sont des entiers.

Mais la substitution

$$x = rx_1 + sy_1, \qquad y = -tx_1 - uy_1$$

est une substitution unité qui fait passer de la forme I à la forme $Ax_1^2 + 2Bx_1y_1 + Cy_1^2$. Le théorème est démontré.

On pourrait faire voir, de la même manière, que la forme II est

équivalente à toute forme de déterminant m qui peut représenter $-p$.

On pourrait trouver les mêmes résultats en partant de la forme $\mathfrak{p} = (p, b + \sqrt{m})$ des idéaux principaux et en procédant comme il suit.

Idéaux premiers et formes quelconques.

Soit p un nombre premier, tel que $\left(\frac{d}{p}\right) = +1$ ou $\left(\frac{d}{p}\right) = 0$, et supposons que (p) se décompose dans $k(\sqrt{m})$ en un produit de deux idéaux du premier degré, idéaux principaux ou non principaux, ou supposons encore que (p) soit le carré d'un idéal, on peut écrire

$$(p) = \mathfrak{p} \cdot \mathfrak{p}' = (p, b + \sqrt{m})\,(p, b - \sqrt{m}),$$

où b est un nombre positif, qui peut être nul.

On pourra attribuer des formes de déterminant D aux idéaux $\mathfrak{p}$ et $\mathfrak{p}'$. Par définition à l'idéal $\mathfrak{p}$ correspondent

$$f = \frac{1}{p}(px + by + \sqrt{m}y)(px + by - \sqrt{m}y),$$

c'est-à-dire

$$\text{(I)} \qquad f = px^2 + 2bxy + \frac{b^2 - m}{p}y^2$$

ou

$$\text{(II)} \qquad f = -px^2 + 2bxy + \frac{b^2 - m}{p}y^2,$$

et à $\mathfrak{p}'$

$$\text{(III)} \qquad f = px^2 + 2bxy + \frac{b^2 - m}{p}y^2,$$

$$\text{(IV)} \qquad f = -px^2 + 2bxy - \frac{b^2 - m}{p}y^2.$$

Il faut remarquer que toutes ces formes sont proprement primitives, car les coefficients n'ont aucun facteur commun ; de plus.

a) Les formes I et III d'une part, II et IV d'autre part, sont

improprement équivalentes, car elles se déduisent l'une de l'autre par la substitution

$$x = x_1, \qquad y = -y_1$$

de déterminant -1.

b) Pour des valeurs données des entiers x et y, les formes I et II ou III et IV nous donnent des nombres égaux et de signes contraires.

Dans le cas où la norme de l'unité fondamentale ε, $n(\varepsilon) = -1$, les formes I et II, III et IV sont aussi improprement équivalentes, car si $\varepsilon = r + s\sqrt{m}$, la transformation

$$x = (r - bs)x_1 - \frac{b^2 - m}{p} sy_1$$
$$y = + psx_1 + (r + bs)y_1,$$

dont le déterminant est -1, fait passer de I à II et de III à IV. On peut réunir les remarques *a*) et *b*) et dire que si $n(\varepsilon) = -1$, les formes I, IV, II, III sont proprement équivalentes, et la forme $\left\{\begin{matrix}\text{I}\\ \text{IV}\end{matrix}\right.$ est improprement équivalente à la forme $\left\{\begin{matrix}\text{II}\\ \text{III}\end{matrix}\right.$.

c) Dans le cas où $\mathfrak{p}$ est un idéal ambige, c'est-à-dire si

$$(p, b + \sqrt{m}) = (p, b - \sqrt{m}) = (p, b + \sqrt{m}, b - \sqrt{m}),$$

on peut trouver deux entiers r_1, s_1, tels que

$$pr_1 + (b + \sqrt{m})s_1 = b - \sqrt{m},$$

c'est-à-dire

$$s_1 = -1, \qquad pr_1 - b = b,$$

c'est-à-dire

$$r_1 = \frac{2b}{p}.$$

Alors III résulte de I par

$$x = x_1 - \frac{2b}{p} y, \qquad y = y_1,$$

dont le déterminant est $+1$. Les formes I et III sont donc alors proprement équivalentes ainsi que II et IV.

Si donc $n(\varepsilon) = +1$ nous ne conserverons que les formes I et II,

si $n(\varepsilon) = -1$ il résulte des remarques b) et c) que les quatre formes de I à IV sont équivalentes et peuvent être remplacées par une seule d'entre elles.

La forme I est équivalente à III, proprement et improprement, elle est donc improprement équivalente à elle-même.

En effet, la substitution

$$x = x_1 + \frac{2b}{p} y_1, \qquad y = -y_1, \qquad \Delta = -1,$$

ne la transforme pas. Des formes telles que I, II, III, IV, dans le cas considéré, qui sont leur propre équivalent, proprement et improprement, sont dites des formes ambiges (d'après Dedekind), ou formae ancipides (Gauss).

d) Enfin si $\mathfrak{p}$ est un idéal principal, on a le cas précédent, les formes (I, III), (II, IV) sont équivalentes à l'une des formes $x^2 - my^2$ ou $-x^2 + my^2$, ou encore à toutes les deux.

Les formes I et III sont encore équivalentes entre elles, proprement et improprement, chacune d'elles est improprement équivalente à elle-même. Les formes I, II sont des formes ambiges.

Des transformations unités nous permettent de déduire de ces formes une infinité de formes équivalentes.

Dans le cas général on arrive à quatre systèmes de formes, dans certains cas on en a deux, dans d'autres un seul.

Tout nombre rationnel $\pm z$ qui peut être représenté par l'une des formes de I à IV peut être représenté par toutes les formes équivalentes. Réciproquement, toute forme f de déterminant m qui peut représenter proprement un nombre premier p, positif ou négatif, est équivalente à l'une des formes de I à IV.

Soit par exemple

$$+ p = Ax_1^2 + 2Bx_1y_1 + Cy_1^2,$$

x_1 et y_1 étant premiers entre eux, on peut trouver deux nombres entiers s et u tels que

$$x_1u - y_1s = +1,$$

la substitution

$$x = x_1x' + sy'$$
$$y = y_1x' + uy'$$

transforme f en

$$F = +px'^2 + 2\{(Ax_1 + By_1)s + (Bx_1 + Cy_1)u\}x'y' + (As^2 + 2Bsu + Cu^2)y'^2.$$

ou encore

$$F = +px'^2 + 2b_1x'y' + c_1y'^2.$$

Le déterminant de cette forme est égal à m, il en résulte

$$c_1 = \frac{b_1^2 - m}{p}.$$

c'est-à-dire

$$b_1^2 - m \equiv 0\ (p).$$

b_1 est donc un entier rationnel qui satisfait à $X^2 - m \equiv 0\ (p)$. Nous montrerons plus loin que le nombre b_1 ne dépend, suivant le module p, que de x_1 et y_1, et qu'il ne dépend pas des valeurs particulières choisies pour u et s.

Le nombre b satisfaisant à la même congruence, et comme cette congruence n'a que deux racines distinctes suivant le module (p), ou une seule dans le cas de $m \equiv 0\ (p)$.

On a : $b_1 = \pm b + ep$, e étant un entier positif ou négatif; posons $x' = X - eY$, $y' = Y$, il vient

$$F_1 = pX^2 \pm 2bXY + (pe^2 + c_1)Y^2.$$

$$F_1 = pX^2 \pm 2bXY + (pe^2 + c_1 \pm 2be)Y^2.$$

dont le déterminant

$$b^2 - p \pm 2bc(pe^2 + c_1) = m.$$

et l'on peut écrire

$$F_1 = pX^2 \pm 2bXY + \frac{b^2m}{p}Y^2.$$

qui n'est autre que la forme I ou III, attribuée aux idéaux $\mathfrak{p}$ et $\mathfrak{p}'$.

On peut résumer ainsi les considérations précédentes :

Soit $\mathfrak{p} = (p, b + \sqrt{m})$, ou encore $\mathfrak{p}' = (p, b - \sqrt{m})$, un idéal premier du corps $k(\sqrt{m})$, où b est positif ou nul, nous attribuerons aux idéaux $\mathfrak{p}$ et $\mathfrak{p}'$:

A. Les formes I, II, respectivement III, IV, si $n(\varepsilon) = -1$, et si $\mathfrak{p}$ n'est ni un idéal principal ni un idéal ambige ;

B. La forme quadratique I, respectivement III, si $n(\varepsilon) = -1$, et si $\mathfrak{p}$ n'est ni un idéal ambige ni un idéal principal.

Mais si $\mathfrak{p}$ est un idéal ambige ou un idéal principal, les formes I, III d'une part, II, IV d'autre part, se confondent, elles sont des formes ambiges.

Si l'on part de l'idéal $(1, \omega)$ ce théorème nous donne les formes attribuées aux idéaux principaux.

Remarque : Il n'était pas nécessaire du tout, pour établir ces correspondances, de prendre pour point de départ la base normale de l'idéal p, $b + \omega$, on pourrait tout aussi bien partir d'une base quelconque donnée.

Soit $\mathfrak{p}$ un idéal premier qui divise p, et soient $\pi = a_1 + b_1\omega$, $\pi_1 = c_1 + d_1\omega$ une base de l'idéal.

On obtiendrait, au lieu des quatre formes I à III, quatre formes analogues, la suivante correspond aux formes I et III,

$$F = \frac{1}{p}\left[(a_1x + c_1y) + (b_1x + d_1y)\omega\right]\left[(a_1x + c_1y) - (b_1x + d_1y)\omega\right]$$

ou

$$(\mathrm{I}_a) \qquad F = \frac{a_1^2 - b_1^2m}{p}x^2 + 2\frac{a_1c_1 - b_1d_1m}{p}xy + \frac{c_1^2 - d_1^2m}{p}y^2.$$

Les coefficients de ces formes n'ont pas de facteur commun, car

$$a_1^2 - b_1^2m, \qquad a_1c_1 - b_1d_1m, \qquad c_1^2 - d_1^2m$$

sont des nombres rationnels de l'idéal $\mathfrak{p}$, et les nombres extrêmes ne peuvent, d'après l'hypothèse, être divisibles que par p^1. De plus, le déterminant $D = m$, car si π, π_1 sont deux nombres de base de l'idéal $\mathfrak{p}$, on peut désigner quatre entiers rationnels r, s, t, u, tels que $ru - st = \pm 1$, et que

$$\pi = rp + t(b + \omega),$$
$$\pi_1 = sp + u(b + \omega).$$

On peut donc écrire

$$F = \frac{1}{p}\cdot n[p(rx + sy) + (tx + uy)b + (tx + uy)\omega].$$

ce qui nous montre que la transformée de F par la substitution

$$x_1 = rx + sy, \qquad y_1 = tx + uy,$$

n'est autre que I ou III, c'est-à-dire que F est équivalente à l'une de ces formes, suivant que $rs - tu$ égale $+1$ ou -1. Le déterminant de F est donc bien égal à m.

Et on a :

Théorème. — On peut faire correspondre, aux différents couples de nombres qui forment une base de l'idéal $\mathfrak{p}$, des formes de déterminant m équivalentes entre elles, proprement ou improprement.

Les idéaux quelconques et les formes.

Soit enfin $\mathfrak{j} = (i_1, i_2)$ un idéal quelconque, et supposons que $\mathfrak{j}$ ne soit pas divisible par un nombre rationnel, on peut poser $i = a$, $i_2 = b + \omega$, où a le plus petit entier rationnel de $\mathfrak{j}$. En effet, si a, $b + c\omega$ est une base de l'idéal, a, b, c ne peuvent avoir aucun facteur commun, sans quoi l'idéal $(\mathfrak{j})$ contiendrait lui-même ce facteur. On peut alors trouver trois entiers rationnels x^*, y^*, z^*, tels que

$$a\omega x^* + by^* + c\omega^* y + cmz^* + bz\omega^*$$

soit de la forme $B + \omega$, ce que nous voulions démontrer.

Soit, dès lors, $\mathfrak{j} = (a, b + \sqrt{m})$, on peut faire correspondre aux deux idéaux $\mathfrak{j}$ et $\mathfrak{j}'$ des formes en général 4 (2 à chacun d'eux), de déterminant m, analogues aux formes de I à IV. A l'idéal $\mathfrak{j}$ correspond, par exemple, la forme

$$f = ax^2 + 2bxy + \frac{b^2 - m}{a} y^2.$$

Tandis qu'il est évident que le nombre $\pm a$ est représentable par la forme f et les trois autres, et par toute forme qui est équivalente à l'une des quatre, il n'est pas possible de démontrer que toute forme de déterminant m qui peut représenter $\pm a$, est toujours équivalente à l'une des quatre formes attribuées à $\mathfrak{j}$ et $\mathfrak{j}'$.

Tout d'abord il y a d'autres idéaux que $\mathfrak{j}$, dont la norme est a, et qui ne sont pas équivalents à $\mathfrak{j}$, et de chacun de ces idéaux

on peut déduire une nouvelle série de quatre formes quadratiques. D'autre part, soit

$$F = Ax^2 + 2Bxy + Cy^2$$

une forme quadratique de déterminant m, qui permet de représenter $+a$ lorsqu'on remplace x, y par les nombres x_1, y_1 premiers entre eux,

$$a = Ax_1^2 + 2Bx_1y_1 + Cy_1^2,$$

déterminons s et u entiers, tels que $x_1u - y_1s = 1$, la transformation unité

$$x = x_1X + sY$$
$$y = y_1X + uY,$$

nous donne

$$F' = aX^2 + 2b_1XY + c_1Y^2.$$

La forme F' ne peut être équivalente à F que si $b_1 \equiv b\ (a)$, comme il est facile de s'en convaincre. Pour voir si F' et f sont équivalents, voyons comment b_1 dépend des nombres x_1, y_1, u, s.

Le déterminant de la forme F' est $b_1^2 - ac_1 = m$, b est donc une racine de l'équation $x^2 - m \equiv 0\ (a)$. Une pareille congruence ne peut avoir que deux racines distinctes, mod. (a), si a est premier, elle peut en avoir plus de deux si a ne l'est pas. Nous allons montrer que b_1 ne dépend, suivant le mod. (a), que de x_1 et y_1, et qu'il ne change pas lorsque u et s sont remplacés par une autre solution de $ux_1 - sy_1 = b$, soit aussi $u_1x - s_1y_1 = 1$, c'est-à-dire

$$(u - u_1)x_1 - (s - s_1)y_1 = 0,$$

ou encore

$$u - u_1 = ky_1, \qquad s - s_1 = kx_1,$$

on a

$$b_1 = Ax_1s + B(x_1u + y_1s) + Cy_1u$$
$$b_2 = Ax_1s_1 + B(x_1u_1 + y_1s_1) + Cy_1u_1,$$

d'où

$$b_1 - b_2 \equiv 0\ (a).$$

On peut donc dire, suivant une expression de Gauss, que la

représentation de a par F, au moyen de x_1, y_1, appartient à une racine déterminée b_1 de la congruence $x^2 - m \equiv 0$.

D'où le *théorème*.

La condition nécessaire et suffisante pour que F soit équivalente à f, est que la représentation de a par F appartienne à la racine b de la congruence $x^2 - m \equiv 0 \ (a)$.

Enfin si $\mathfrak{j}$ est idéal qui est divisible par un nombre rationnel z, on fait la division $\frac{\mathfrak{j}}{z}$ et on attribue à cet idéal simplifié une forme de déterminant $D = m$.

On peut au contraire attribuer à la forme primitive

$$ax^2 + 2bxy + cy^2,$$

de déterminant m, l'idéal $(a, b + \sqrt{m})$ du corps, et alors à des formes équivalentes on pourra faire correspondre un seul et même idéal (voir plus loin).

2[e] *Cas.* — Soit le corps imaginaire $k(\sqrt{m})$ et $m \equiv 2$, $m \equiv 3 \ (4)$, on a encore $d = 4m$; $1, \omega = \sqrt{m}$ est une base et $h \geqslant 1$.

Soit p un nombre premier rationnel, pour lequel $\left(\frac{d}{p}\right) = -1$, qui ne se décompose pas dans le corps $k(\sqrt{m})$, le nombre p n'est représentable par aucune forme quadratique de déterminant $D = m$.

Soit

$$f = ax^2 + 2bxy + cy^2 = \frac{1}{a}\left[(ax + by)^2 - my^2\right],$$

une forme dont le déterminant m est négatif, a et c ont nécessairement le même signe, et f ne peut représenter que des nombres positifs ou des nombres négatifs, suivant que a, c sont positifs ou négatifs. Une pareille forme dont les coefficients extrêmes sont positifs est dite une forme positive, une forme négative lorsque a et c sont négatifs.

Il suffit de considérer soit les unes soit les autres, car ces deux espèces sont bien distinctes, mais elles se comportent de la même manière.

D'après cela, quand on établira la correspondance entre les formes et les idéaux, le seul changement à introduire sera de se limiter d'avance aux formes (I) et (III).

3e *Cas*. — $k(\sqrt{m})$ est un corps réel, tel que $m \equiv 1$ (4).

Si l'on établit la correspondance entre les idéaux et les formes, de la manière précédente, on arrive à des résultats qui ne s'accordent pas avec la théorie de Gauss.

Soit $k(\sqrt{m})$ un pareil corps réel, on peut prendre pour base $1, \omega = \frac{1+\sqrt{m}}{2}$ et dont le discriminant $d = m$. D'après nos conventions antérieures on attribuerait à un idéal $\mathfrak{p} = (a + b\omega)$ une forme comme la suivante

$$f = x^2 + xy + \frac{1-m}{4} y^2.$$

Cette forme ne répond pas à la convention fixée par Gauss et par les autres mathématiciens, que le coefficient moyen est pair. Tandis que dans le premier et le second cas le déterminant des formes $D = m = \frac{1}{4} d$, on aurait ici

$$D = \frac{1}{4} - \frac{1-m}{4} = \frac{m}{4},$$

le déterminant serait fractionnaire.

Des raisons historiques justifient le désir d'attribuer à des idéaux du corps $k(\sqrt{m})$ des formes de déterminant m, conformément à la théorie de Gauss.

Auparavant nous ferons une remarque sur les coefficients d'une forme de déterminant m et sur les nombres représentés par une pareille forme.

Soit

$$f = ax^2 + 2bxy + cy^2,$$

une forme quadratique, telle que

$$D = b^2 - ac = m \equiv 1 \ (4),$$

si les coefficients a, $2b$, c n'ont pas de diviseur commun, en particulier le facteur 2, f ne peut représenter aucun nombre simplement pair, c'est-à-dire un nombre qui contient le facteur 2 et ne contient pas le facteur 4, car si a est impair on a

$$af = (ax + by)^2 - my^2,$$

on en conclut que $a.f$, et par suite f est impair, ou qu'il est divisible au moins par 4. Un nombre simplement pair ne peut donc être représenté par une forme telle que f, que si a, $2b$, c sont divisibles par 2^1.

Lorsque $D \equiv 1$ (4) et que D ne contient pas de facteur au carré, et dans ce cas-là seulement, il existe, outre les formes proprement primitives, des formes dont les coefficients a, $2b$, c sont divisibles par 2^1 et non par d'autres nombres, par exemple

$$2f = 2x^2 + 2xy + 2\frac{1-m}{4}y^2.$$

Gauss dénomme les formes dont tous les coefficients n'ont d'autre diviseur commun que 2^1, des formes improprement primitives de déterminant $D = m$. Comme aucune substitution ne transforme une forme improprement primitive en une forme proprement primitive, il faut distinguer ici les deux espèces de formes.

Tout d'abord on peut attribuer *par définition* à l'idéal $\mathfrak{p}$, non pas la forme f, mais d'autres formes, par exemple la forme improprement primitive

$$2f = 2x^2 + 2xy + 2\frac{1-m}{4}y^2,$$

et aussi les formes proprement primitives, dont le coefficient moyen est pair, qui résultent de f (et des formes analogues à f, formes analogues étant construites comme dans les exemples précédents) par une substitution de déterminant 2, qui ne sont ni équivalentes entre elles ni à $2f$.

Les substitutions

(A) $\begin{cases} x = x_1 \\ y = 2y_1 \end{cases}$ (B) $\begin{cases} x = -2y_1 \\ y = x_1 \end{cases}$ (C) $\begin{cases} x = x_1 + 2y_1 \\ y = -x_1, \end{cases}$

permettent de déduire ces dernières formes de f.

En les joignant à $2f$ on obtient ainsi quatre formes, on ne conservera, comme représentant d'une catégorie de formes, que celles qui ne sont pas équivalentes entre elles.

On obtient de la même manière pour tous les idéaux, principaux et non principaux, une série de formes, dont le coefficient moyen est pair et dont le déterminant est m.

Remarque. — Nous ne démontrerons pas (ce serait facile de le faire) que toute substitution de déterminant 2 se déduit de l'une des substitutions précédentes de déterminant 2, suivie d'une substitution unité.

Car soit

$$x = r_1 x^* + s_1 y^*, \qquad y = t_1 x^* + u_1 y^*$$

une substitution telle que

$$r_1 u_1 - s_1 t_1 = 2 \qquad \text{et} \qquad x^* = r x_1 + s y_1, \qquad y^* = t x_1 + u y_1,$$

une substitution telle que $ru - st = 1$, la substitution résultante

$$x = (r_1 r + s_1 t) x_1 + (r_1 s + s_1 u) y_1$$
$$y = (t_1 r + u_1 t) x_1 + (t_1 s + u_1 u) y_1,$$

est une substitution de déterminant 2.

Réciproquement soit

$$x = \mathrm{R} x_1 + \mathrm{S} y_1, \qquad y = \mathrm{T} x_1 + \mathrm{V} y_1,$$

une substitution quelconque de déterminant 2.

On peut déterminer des entiers r, s, t, u avec $ru - st = 1$, et tels que

$$\mathrm{R} = r_1 r + s_1 t, \text{ etc.},$$

où r_1, s_1, t_1, u_1 sont des coefficients des substitutions (A), (B) ou (C).

Il n'est pas nécessaire de pousser plus loin cette méthode.

Il est plus utile, en effet, de partir de l'anneau $r(\sqrt{m})$ du corps $k(\sqrt{m})$ pour établir les formes proprement et improprement primitives, le dernier cas présente alors peu de différence avec les deux premiers.

Soit $\mathfrak{p} = (a + b\omega)$ un idéal principal du corps, on considérera

$$(2)\, \mathfrak{p} = (2a + 2b\omega),$$

et on lui fera correspondre les formes improprement primitives

(I) $$f = 2x^2 + 2xy + 2\,\frac{1 - m}{4}\,y^2,$$

(II) $$f = -2x^2 - 2xy - 2\,\frac{1 - m}{4}\,y^2.$$

Si de plus $\mathfrak{p} = (a + b\sqrt{m})$ est un idéal principal de l'anneau $r(\sqrt{m})$, on lui fera correspondre les formes proprement primitives

$$\text{I)} \qquad f = x^2 - my^2,$$

$$\text{II)} \qquad f = -x^2 + my^2.$$

On fait ensuite les mêmes considérations que dans le 1ᵉʳ cas. On voit d'abord que les formes I et II sont ambiges, elles ne changent pas si on fait

$$x = -x_1 - y_1, \qquad y = y_1.$$

D'une façon générale, une forme improprement primitive n'est jamais équivalente à une forme proprement primitive, on le constate en faisant une substitution unité.

Autrement dit les formes I et II correspondent à l'idéal $(2, 2\omega)$ du corps, les autres à l'idéal $(1, \sqrt{m})$ de l'anneau $r(\sqrt{m})$.

Soit $\mathfrak{p}$ un idéal premier quelconque du corps premier avec (2), et on attribue aux idéaux $(2)\mathfrak{p}$, $(2)\mathfrak{p}'$ quatre formes improprement primitives, et aux idéaux d'anneaux réguliers $\mathfrak{p}_r$, $\mathfrak{p}_r'$ correspondants on attribue quatre formes proprement primitives, exactement comme dans les cas précédents.

On étudie chacun de ces groupes de quatre séries comme on l'a fait précédemment, l'introduction des deux espèces de formes primitives constitue la différence essentielle.

Enfin le

4ᵉ *Cas*. — Où $k(\sqrt{m})$ est un corps imaginaire, et $m \equiv 1\ (4)$ ne se distingue du précédent, qu'en ce que dès l'abord on peut se contenter d'étudier soit les formes positives, soit les formes négatives de déterminant $D = m$.

37. — La multiplication des idéaux et la composition des formes. — Nous avons défini la correspondance entre les idéaux et les formes, et réciproquement, c'est là la base de la théorie des formes quadratiques. Il nous faut savoir maintenant quels sont les rapports entre les classes d'idéaux et les classes de formes.

Ils dépendent de la question suivante :

Comment appliquerons-nous la multiplication des idéaux à des opérations sur les formes?

Ici encore il faudrait distinguer les deux cas $m \equiv 1\ (4)$ et

$m \not\equiv 1\ (4)$. Nous ne traiterons que $m \equiv 2$, $m \equiv 3, (4)$ laissant au lecteur le soin d'étudier le second.

Soient $\mathfrak{p}$ et $\mathfrak{q}$ deux idéaux premiers différents, équivalents ou non du corps $k(\sqrt{m})$, et soit

$$\mathfrak{p} = (p,\ b + \sqrt{m}), \qquad \mathfrak{q} = (q,\ b_1 + \sqrt{m}),$$

le produit $\mathfrak{pq}$ est encore un idéal du corps, que l'on peut écrire

$$\mathfrak{pq} = (pq,\ \mathrm{B} + \sqrt{m}).$$

Le nombre entier $\mathrm{B} + \sqrt{m}$ appartient à l'idéal $\mathfrak{p}$ et à l'idéal $\mathfrak{q}$, c'est-à-dire qu'il existe deux entiers u et v tels que

$$pu + b = \mathrm{B}, \qquad qv + b_1 = \mathrm{B},$$

et l'on peut prendre p, $\mathrm{B} + \sqrt{m}$ comme nombres de base de $\mathfrak{p}$, et q, $\mathrm{B}\sqrt{m}$ comme nombres de base de $\mathfrak{q}$, par suite, les formes attribuées à $\mathfrak{p}$, $\mathfrak{q}$, $\mathfrak{pq}$ sont

$$(1) \qquad f = px^2 + 2\mathrm{B}xy + \frac{\mathrm{B}^2 - m}{q}y^2,$$

$$(2) \qquad f_1 = qx^2 + 2\mathrm{B}xy + \frac{\mathrm{B}^2 - m}{pq}y^2,$$

$$(3) \qquad \mathrm{F} = pq\mathrm{X}^2 + 2\mathrm{BXY} + \frac{\mathrm{B}^2 - m}{pq}\mathrm{Y}^2.$$

Ces trois formes sont entre elles, dans un rapport remarquablement simple, comme nous allons le montrer.

En effet, comme $px + (\mathrm{B} + \sqrt{m})y$ est un nombre de l'idéal $\mathfrak{p}$, et que $qx_1 + (\mathrm{B} + \sqrt{m})y$ et $py\mathrm{X} + (\mathrm{B}\sqrt{m})\mathrm{Y}$ sont des nombres de l'idéal $\mathfrak{q}$ et de l'idéal $\mathfrak{pq}$, le théorème relatif à la multiplication des idéaux nous apprend que

$$[px + (\mathrm{B} - \sqrt{m})y]\,[qx_1 + (\mathrm{B} + \sqrt{m})y] = pq\mathrm{X} + (\mathrm{B} + \sqrt{m})\mathrm{Y},$$

d'où

$$(\Sigma) \qquad \begin{cases} \mathrm{X} = xx_1 - \dfrac{\mathrm{B}^2 - m}{p \cdot q}yy_1, \\ \mathrm{Y} = pxy_1 + qx_1y + 2\mathrm{B}yy_1. \end{cases}$$

On peut donc dire que la forme F se transforme en le produit

des deux formes f et f_1, par la substitution (Σ). Réciproquement, le produit ff_1 égale F, lorsqu'on lie x_1 et y_1, par les relations (Σ).

Si l'on attribuait directement aux idéaux $\mathfrak{p}$ et $\mathfrak{q}$ les formes

$$\varphi = px'^2 + 2bx'y' + \frac{b^2 - m}{p} y'^2,$$
$$\varphi_1 = px_1'^2 + 2b_1x_1'y_1' + \frac{b_1^2 - m}{q} y_1'^2,$$

F peut encore être considéré comme le produit de φ et de φ_1. En effet φ est équivalent à f, et φ_1 est équivalent à f_1, et on voit que notre proposition est vraie, en faisant dans (Σ)

$$x = x' + uy', \qquad x_1 = x_1' + vy_1',$$
$$y = y', \qquad y_1 = y_1'.$$

Gauss a introduit le mot de composition des formes. La forme F est dite composée des formes f et f_1, on l'écrit symboliquement

$$\mathrm{F} = f \cdot f_1.$$

La composition reste évidemment la même lorsque $\mathfrak{p}$ et $\mathfrak{q}$ sont deux idéaux ambiges premiers différents. On voit, de plus, ce qui se passe pour les formes attribuées aux idéaux $\mathfrak{p}$ et $\mathfrak{p}^2$. Soit $\mathfrak{p}$ un idéal premier qui ne divise pas (2)

$$\mathfrak{p} = (p, \mathrm{B} + \sqrt{m}), \qquad \mathfrak{p}^2 = (p^2, \mathrm{B} + \sqrt{m}),$$

soit alors

$$f = px^2 + 2\mathrm{B}xy + \frac{\mathrm{B}^2 - m}{p} y^2,$$
$$\mathrm{F} = p^2\mathrm{X}^2 + 2\mathrm{BXY} + \frac{\mathrm{B}^2 - m}{p^2} y^2,$$

les formes qui leur correspondent, on voit que l'on peut poser $\mathrm{F} = f^2$, si X, Y et x, y sont liés par

$$(\Sigma_1) \qquad \begin{cases} \mathrm{X} = x^2 - \dfrac{\mathrm{B}^2 - m}{p^2} y^2, \\ \mathrm{Y} = 2pxy + 2\mathrm{B}y^2. \end{cases}$$

On dit alors que la forme F est composée avec elle-même, et en comparant les substitutions (Σ) et (Σ_1), que le cas particulier peut se déduire du cas général.

Une telle composition n'est impossible que si $\mathfrak{p}$ divise (2), par contre, si $\mathfrak{p}$ est un idéal ambige premier avec (2), on peut écrire

$$\mathfrak{p} = (p, \sqrt{m}), \qquad \mathfrak{p}^2 = (p, p\sqrt{m}),$$

par suite

$$f = px^2 - \frac{m}{p} y^2,$$
$$F = X^2 - mY^2,$$

et on a $F = f^2$ pour

$$X = px^2 + \frac{m}{y} y^2,$$
$$Y = 2xy.$$

Reste à savoir comment l'on peut composer deux formes qui correspondent à deux idéaux quelconques $\mathfrak{j}$ et $\mathfrak{j}'$ du corps,

$$\mathfrak{j} = (a, b + c\sqrt{m}),$$
$$\mathfrak{j}_1 = (a_1, b_1 + c\sqrt{m}).$$

Nous admettrons d'abord que ces idéaux ne sont divisibles par aucun idéal principal, de sorte que les formes correspondantes n'aient pas de facteur commun. Il faut alors que a, b, c soient premiers dans leur ensemble, ainsi que a_1, b_1, c_1.

On peut alors mettre les idéaux sous la forme

$$\mathfrak{j} = (a, b + \sqrt{m}), \qquad \mathfrak{j}_1 = (a_1, b_1 + \sqrt{m}),$$
$$\mathfrak{j}\mathfrak{j}_1 = (aa_1, a_1 b + a_1\sqrt{m}, \quad ab_1 + a\sqrt{m}, \quad bb_1 + m + (b + b_1)\sqrt{m}, \ldots),$$

et l'on pourra choisir une base

$$aa_1, \qquad B + \sqrt{m},$$

c'est-à-dire

$$\mathfrak{j}\mathfrak{j}_1 = (aa_1, B + \sqrt{m}),$$

si a, a_1, $b + b_1$ n'ont pas de facteur commun. Nous supposerons que cette condition est remplie.

On peut alors poser

$$\mathfrak{j} = (a, B + \sqrt{m}), \qquad \mathfrak{j}_1 = (a_1, B + \sqrt{m}),$$

car il existe deux entiers u et v, tels que

$$B = au + b = a_1 v + b_1,$$

faisons correspondre à $\mathfrak{j}$, $\mathfrak{j}_1$ et $\mathfrak{j}\mathfrak{j}_1$ les formes

$$f = ax^2 + 2\,Bxy + \frac{B^2 - m}{a}\,y^2,$$

$$f_1 = a_1 x_1^2 + 2\,Bx_1 y_1 + \frac{B^2 - m}{a_1}\,y_1^2,$$

$$F = aa_1 X^2 + 2\,BXY + \frac{B^2 - m}{aa_1}\,Y^2,$$

F peut encore être représenté comme le produit de f et de f_1, car d'après la multiplication des idéaux

$$[ax + By + \sqrt{m}y]\,[a_1 x_1 + By_1 + \sqrt{m}y_1] = aa_1 X + (B + \sqrt{m})Y,$$

d'où

$$(\Sigma_2) \qquad \begin{cases} X = xx_1 - \dfrac{B^2 - m}{aa_1}\,yy_1, \\ Y = axy_1 + a_1 x_1 y + 2\,Byy_1. \end{cases}$$

Si l'on remplace X et Y par ces valeurs dans F, on obtient le produit ff_1.

Si l'on attribue aux idéaux $\mathfrak{j}$ et $\mathfrak{j}_1$, au lieu de f et de f_1, les formes

$$\varphi = ax'^2 + 2\,bx'y' + \frac{b^2 - m}{a}\,y'^2$$

$$\varphi_1 = a_1 x_1'^2 + 2\,b_1 x_1' y_1' + \frac{b_1^2 - m}{a_1}\,y_1'^2$$

correspondant aux représentations primitives $\mathfrak{j} = (a,\ b + \sqrt{m})$ et $\mathfrak{j}_1 = (a_1,\ b_1 + \sqrt{m})$, f et φ, f_1 et φ_1 sont équivalents, et on voit comme il a été fait pour les idéaux premiers $\mathfrak{p}$ et $\mathfrak{q}$, que F peut être représenté comme le produit de φ et de φ_1.

Réunissant tous les résultats obtenus, nous voyons que deux formes de même déterminant

$$f = ax^2 + 2\,bxy + cy^2$$
$$f_1 = a_1 x_1^2 + 2\,b_1 x_1 y_1 + c_1 y_1^2,$$

peuvent toujours être composées en une forme F, de même déterminant, lorsque a, a_1, $b + b_1$ n'ont pas de diviseur commun.

Une remarque s'impose, non seulement la forme F, mais toute forme équivalente F', équivalente à F, peut être composée de f et de f_1.

On peut inverser ce que nous avons fait et dire, si la forme F est composée des deux formes f et f_1, et si les idéaux $\mathfrak{j}\mathfrak{j}_1$ correspondent à f et f_1, l'idéal correspondant à F est $\mathfrak{j}\mathfrak{j}_1$.

D'après Gauss, le théorème fondamental de la composition des formes est le suivant :

Théorème. — Si des deux formes f et f_1 on peut composer la forme F, et si des deux formes φ et φ_1 on peut composer Φ, f étant équivalent à φ, f_1 à φ_1, il est certain que F est équivalent à Φ.

Démonstration : Supposons que a soit représentable par f, et que a_1 le soit par f_1, ils le seront aussi respectivement par φ et par φ_1. aa_1 peut alors être représenté à la fois par F et par Φ. D'après le théorème qui suit (et que nous plaçons à la suite de celui-ci pour des raisons d'ordre pratique), aux formes f et φ, f_1 et φ_1 correspondent des idéaux équivalents. Soient $\mathfrak{j}$ et $\mathfrak{h}$ correspondant à f et φ, $\mathfrak{j}_1$ et $\mathfrak{h}_1$ correspondant à f_1 et φ_1,

$$\mathfrak{j} \sim \mathfrak{h}, \qquad \mathfrak{j}_1 \sim \mathfrak{h}_1,$$

et par suite

$$\mathfrak{j}\mathfrak{j}_1 \sim \mathfrak{h}\mathfrak{h}_1.$$

Aux idéaux $\mathfrak{j}\mathfrak{j}_1$ et $\mathfrak{h}\mathfrak{h}_1$ correspondent les formes F et Φ, qui sont proprement équivalentes, car elles peuvent être représentées à la fois par des nombres positifs et par des nombres négatifs.

Le rapport entre la composition des formes et la multiplication des idéaux, nous donne comme conséquence la plus importante, le rapport entre les classes de formes et les classes d'idéaux, comme il ressort du théorème suivant :

Théorème. — Soient $\mathfrak{j}$ et $\mathfrak{j}_1$ deux idéaux équivalents du corps $k(\sqrt{m})$, n'ayant ni l'un ni l'autre de facteur rationnel, les formes quadratiques, qui, par définition, correspondent à ces idéaux, sont aussi équivalentes deux à deux.

Démonstration : On peut tout d'abord, en partant de la composition des formes, donner une autre définition de l'équivalence des formes. Soient les deux formes f et f_1, que l'on peut composer avec la même forme principale $\varphi = x^2 - my^2$, de telle sorte que les

deux formes $F = f.\varphi$ et $F_1 = f.\varphi$ soient équivalentes ou égales, les formes f et f_1 sont également équivalentes, et réciproquement. Car alors tout nombre qui est représentable par f l'est aussi par f_1, tout en appartenant à la même racine de la congruence.

$\mathfrak{j}$ et $\mathfrak{j}_1$ étant équivalents, il existe deux entiers du corps α et β, tels que

$$(\alpha)\,\mathfrak{j} = (\beta)\,\mathfrak{j}_1.$$

Si donc on fait correspondre à l'idéal principal (α) la forme φ, et à l'idéal (β) la forme $\pm\varphi$, et si f, f_1, F sont les formes qui correspondent à $\mathfrak{j}$, $\mathfrak{j}_1$ et à $(\alpha)\,\mathfrak{j} = (\beta)\,\mathfrak{j}_1$, on a nécessairement

$$F = \varphi.f = \pm\,\varphi f_1.$$

Et en effet, les formes φ, f d'une part, $\pm\varphi$, f_1 d'autre part, peuvent être composées d'après la règle générale, le coefficient a_1 de φ étant égal à 1. De l'équation $\varphi f = \pm\,\varphi f_1$ il résulte que f et $\pm f_1$ sont équivalentes, c'est-à-dire que les quatre formes attribuées à $\mathfrak{j}$ et $\mathfrak{j}_1$ sont équivalentes deux à deux.

D'autre part, à deux formes équivalentes f et f_1, correspondent des idéaux $\mathfrak{j}$ et $\mathfrak{j}_1$, tels que

$$\mathfrak{j} \sim \mathfrak{j}_1.$$

Ceci montre qu'au nombre fini des classes d'idéaux du corps $k(\sqrt{m})$ correspond un nombre fini de formes quadratiques de déterminant m. Le nombre de ces dernières est au moins égal, en général supérieur, et au plus égal à quatre fois le nombre des classes d'idéaux.

A une classe d'idéaux ambiges correspond toujours une classe de formes avec des formes ambiges. En appliquant aux formes quadratiques le théorème de Minkowski, qui permet la détermination pratique du nombre h des classes d'idéaux, on verrait que : Dans toute classe de forme de déterminant $D = m$ il y a au moins une forme quadratique dont les coefficients satisfont à

$$|b| \leqq |\sqrt{m}|, \qquad |a| \leqq 2\,|\sqrt{m}|, \qquad |a| \geqq |c|.$$

Gauss a donné le nom de *formes réduites* aux formes dont les coefficients satisfont à ces inégalités.

Les unités d'un corps jouent un rôle particulièrement important

dans les formes quadratiques ; elles fournissent toutes les transformations propres ou impropres d'une forme en elle-même, et, de plus, toutes les transformations d'une forme f en une forme f_1, lorsqu'on connaît *une* transformation qui fait passer de f à f_1. Pour s'en rendre compte, il suffit de se rappeler la constitution d'une forme comme norme de

$$ax + (b + \sqrt{m})y,$$

et de multiplier cette expression par ε^a, on obtient les formules de transformations cherchées.

La représentation d'un nombre par une forme est parallèle à la décomposition du nombre dans le corps.

Nous ne poursuivrons pas les analogies entre la théorie des idéaux et la théorie des formes. Il est évident que toutes les notions de multiplication des classes, répartition des classes en genres, système des caractères d'un genre, etc. s'appliquent.

Nous ne ferons plus qu'une remarque relative à la composition des formes improprement primitives, dont le déterminant $D \equiv 1\ (4)$, on divise les coefficients par 2, on compose les formes et on double les coefficients de la forme ainsi obtenue.

38. — La représentation géométrique des idéaux. — La théorie des idéaux, que nous avons développée par des voies purement arithmétiques, offre des résultats géométriques très intéressants. En effet, on peut représenter les idéaux d'un corps par des images géométriques, qui ont une grande importance en minéralogie, particulièrement en cristallographie, et qui même y sont nécessaires. Dans ce paragraphe nous exposerons les principes de ces considérations géométriques, car son application aux résultats obtenus est déjà fort élégante en elle-même, de plus, elle nous fera voir, sous un jour nouveau, certains faits déjà acquis, et elle justifiera l'étude approfondie du corps quadratique (qui d'ailleurs n'est qu'un cas particulier d'une théorie générale). Ceux qui pensent géométriquement prendront plaisir à cette nouvelle conception des résultats et des méthodes arithmétiques, sans oublier que la recherche des analogies est toujours un excellent principe d'étude scientifique.

Comme dans les démonstrations arithmétiques, nous trouverons une grande différence entre les corps réels et les corps imaginaires.

Nous les étudierons donc séparément, et nous commencerons par les corps imaginaires.

Le lecteur est prié de faire de nombreuses figures.

Nous nous en tiendrons d'abord à un exemple numérique typique pour tous les corps imaginaires, et dont le nombre fondamental $m \not\equiv 1 \pmod 4$. Nous considérerons un corps que nous avons déjà traité souvent $k(\sqrt{-5})$, pour lequel le nombre des classes $h = 2$.

Choisissons deux axes de coordonnées, et adoptons la représentation des imaginaires d'après Gauss. Tout entier du corps $a + b\sqrt{-5}$ est représenté par un point dont l'abscisse est a, l'ordonnée $b\sqrt{5}$.

On peut prendre 1 comme unité de longueur sur Ox, et $\sqrt{5}$ comme unité de longueur sur Oy, les nombres entiers du corps sont alors représentés par les points dont les coordonnées sont mesurées par des entiers, ou encore, comme l'on dit, par les « points entiers » [1].

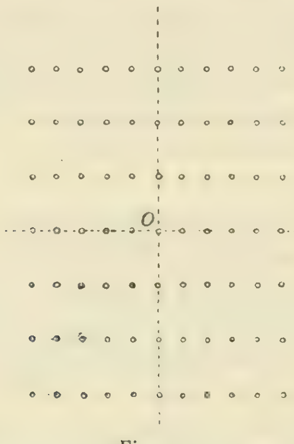


Fig. 1.

La figure formée par l'ensemble de ces points (sans les droites qui les joignent), s'appelle un *réseau régulier de points* (Punktgitter) [2], et un de ces points est dit un *sommet* (*ou un point*) du réseau (Gitterpunkt) [3].

---

[1] Nous exclurons le point à l'infini.

[2] Gauss le 1er a signalé cette représentation géométrique (*Ges. W.*, t. II), puis Lejeune-Dirichlet (*Ges. W.*, t. II, p. 21, p. 29).

[3] Klein a traité ces questions en ce qui concerne leurs applications, *Autogr. Vorlesungen.*

Considérons un double système de parallèles, tel que tout sommet soit l'intersection de deux parallèles, et que deux parallèles voisines soient toujours équidistantes, nous dirons que nous avons formé un *réseau de parallèles*.

Dans l'exemple précédent, les parallèles aux axes forment un réseau de parallèles rectangulaires, et tel que les distances soient 1 et $\sqrt{5}$.

Dans ce qui suit, il ne s'agira que de réseaux de points et de réseaux de parallèles, nous ne commettrons aucune confusion en employant simplement le mot réseau lorsqu'il s'agira des derniers.

Un de ces réseaux partage le plan en une infinité de parallélogrammes. Nous appellerons *parallélogramme élémentaire* ou *maille*

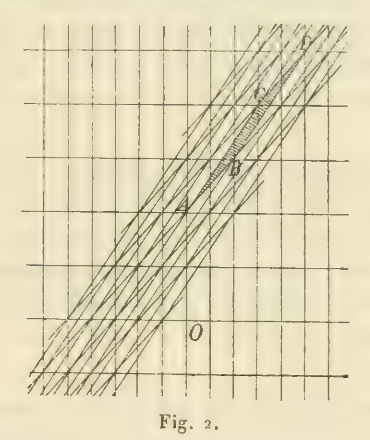


Fig. 2.

du réseau, un parallélogramme qui ne contient aucun point à l'intérieur de son aire. Les mailles recouvrent tout le plan sans discontinuité. Un réseau est parfaitement déterminé par une maille donnée, en grandeur et en position. On a tout d'abord :

Théorème. — On peut faire passer une infinité de réseaux de parallèles par le réseau des points entiers.

Démonstration : (Fig. 2). On part d'un sommet A, et on choisit deux autres sommets B et C, tel qu'il n'y ait pas d'autre point du réseau à l'intérieur du triangle ABC, ni sur ses côtés. Ce choix peut être fixé d'une infinité de manières. Si l'on a choisi B, tel que sur $\overline{AB}$ il n'y ait pas d'autre point du réseau, la ligne qui porte ce segment AB, contient une infinité d'autres points, tels que deux points voisins soient toujours distants de $\overline{AB}$, et en même temps la

ligne AB partage le réseau de points en deux parties, l'une à gauche de AB, l'autre à droite. Il est facile de voir que l'on peut répartir tous les points du réseau sur un système de parallèles à AB, équidistantes entre elles, chacune de ces lignes portant une infinité de points distants entre eux de AB. Sur la parallèle voisine de AB, choisissons deux points voisins quelconques CD, comme $\overline{AB} = \overline{CD}$, la figure ABCD est un parallélogramme qui, par sa construction même, ne peut contenir aucun point du réseau, ni sur ses côtés, ni à l'intérieur. Donnons à ce parallélogramme une série de translations, $\overline{AB}$, puis $\overline{BA}$, on obtient consécutivement tous les points du réseau situés sur AB et sur CD, et la bande située entre ces deux droites est partagée en parallélogrammes. Donnons ensuite à cette bande une suite de translations $\overline{AC}$ et $\overline{CA}$, nous couvrirons tout le plan de parallélogrammes sans aucune lacune, et les sommets ABCD, de tous ces parallélogrammes, coïncident avec des points du réseau.

On voit de plus que ces parallélogrammes peuvent se déduire les uns des autres par des translations parallèles aux axes, et mesurées par des *nombres entiers*. Aucun de ces parallélogrammes ne peut contenir un point du réseau sur ses côtés ou dans son aire. Car si A'B'C'D' contenait un point P', la translation qui amène A'B'C'D' en ABCD amènerait P' en un point P, situé sur les côtés ou à l'intérieur de ce dernier.

Ces translations de la maille ABCD nous fournissent un réseau de droites qui contient tous les points du réseau, et tel que par tous les points du réseau il ne passe une parallèle à AB et une à AC.

Nous ajouterons deux remarques :

1. On obtiendrait exactement le même réseau en partant d'un autre point que A. Tous les points du réseau jouent le même rôle, puisqu'on peut lui donner des translations telles que tout point puisse être amené en A.

2. Une maille détermine le réseau de parallèles, et nous fait obtenir le réseau de tous les points.

L'expression géométrique

$$\overline{AB}x_1 + \overline{AC}y_1,$$

où x_1, y_1 sont des nombres entiers, nous fournit tous les points du

réseau, cela revient à rapporter ce réseau à des axes obliques, x_1, y_1 sont les coordonnées d'un point, les unités de longueur sur les axes étant respectivement AB et AC. Mais les points du réseau ne sont que les images des nombres entiers du corps, et le résultat de cette analyse géométrique n'est autre chose qu'un théorème déjà trouvé entièrement : Dans tout corps, on peut choisir d'une infinité de manières un couple de nombres ω_1, ω_2, tels que

$$\omega_1 x_1 + \omega_2 y_1,$$

où x_1, y_1 sont des entiers rationnels, représente tous les entiers du corps. Soient ω_1, ω_2 deux nombres de base, les quatre points o, ω_1, ω_2, $\omega_1 + \omega_2$ sont les sommets d'une maille, ω_1, ω_2 nous donnent les axes d'un système de coordonnées avec les longueurs unités de ce système.

Soient ω_1^*, ω_2^* deux autres nombres de base, nous avons vu, au début de ce livre, qu'on a

$$\text{(T)} \qquad \begin{cases} \omega_1^* = r\omega_1 + s\omega_2 \\ \omega_2^* = t\omega_1 + u\omega_2, \end{cases}$$

où r, s, t, u sont quatre entiers rationnels satisfaisant à

$$ru - st = \pm 1.$$

Les points o, ω_1^*, ω_2^* déterminent un nouveau système de coordonnées, et soient x, y les nouvelles coordonnées d'un point du système

$$\omega_1^* x + \omega_2^* y = (rx + ty)\omega_1 + (sx + uy)\omega_2,$$

la transformation

$$x = rx_1 + ty_1$$
$$y = sx_1 + uy_1$$

nous permet de passer de l'un des systèmes de coordonnées à l'autre.

La géométrie projective nous apprend que, par rapport aux axes AB, AC, la transformation

$$\text{(S)} \qquad \begin{cases} x_1 = rx + ty \\ y_1 = sx + uy, \end{cases}$$
$$ru - st = \pm 1,$$

n'est autre chose qu'une transformation homographique, telle qu'à tout système de droites parallèles corresponde un autre système de parallèles, et que le rapport des surfaces correspondantes est constant. Tout point, autre que le point zéro, est transformé en un autre point.

Dans la théorie des transformations linéaires, la transformation S est dite corrélative de la transformation T, qui permet de passer d'une base à une autre. On a donc :

Théorème. — La transformation (S) transforme analytiquement le réseau des parallèles ω_1, ω_2 en le réseau ω_1^*, ω_2^*.

Deux transformations linéaires successives donnent comme résultante une transformation unique, dont le déterminant est le produit des déterminants des deux premières. D'où tout réseau de parallèles peut être déduit du réseau rectangulaire, ou de tout autre, par une transformation homographique de déterminant $\pm$ 1.

On démontre facilement, à l'aide du théorème relatif à la multiplication des déterminants, que l'aire d'une maille est toujours égale à $\sqrt{5}$, c'est-à-dire qu'elle est constante pour tous les réseaux.

Géométriquement, nous voyons que le passage d'un réseau à un autre s'obtient par une transformation homographique.

Les cas du déterminant $+ 1$ et $- 1$ se ramènent l'un à l'autre, au moyen d'une symétrie, par rapport à un axe.

Résumons :

Les points d'un réseau correspondent aux nombres entiers d'un corps, dans lequel on peut insérer une infinité de réseaux de parallèles ayant des mailles de même aire. Tout réseau de parallèles correspond à une base du corps. Deux quelconques de ces réseaux sont reliés analytiquement par une transformation homographique de déterminant $\pm$ 1, qui est corrélative de la transformation qui relie entre elles les deux couples de base correspondante.

Nous entendons par somme, différence, produit de deux points du réseau, ce qu'on convient d'appeler ainsi, dans la représentation géométrique des imaginaires. Il en résulte alors :

1. Le produit de deux points du réseau est un point du réseau.

2. La somme, la différence de deux points du réseau est un point du réseau.

Soit dès lors α un entier du corps, l'idéal principal (α) comprend tous les entiers du corps qui sont des multiples de α.

Il s'ensuit que nous représenterons géométriquement l'idéal principal, par l'ensemble des points du réseau qui sont divisibles par α, ou encore, par l'ensemble des points du réseau, obtenus en multipliant les points du corps par α.

Nous allons montrer que ces points forment un réseau de points. Nous dirons que l'ensemble des points du corps forme *le réseau*

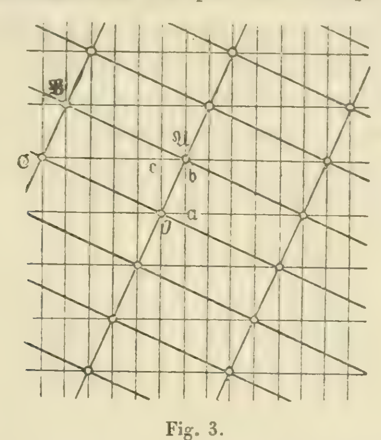


Fig. 3.

fondamental, nous pourrons dire qu'à l'idéal (α) correspond un réseau (α). Voir (*fig.* 3), où l'on a représenté

$$(\alpha) = (1 + \sqrt{5}).$$

Lorsqu'on multiplie par α les points du réseau fondamental situés sur une ligne droite, on obtient des points tous situés en ligne droite.

Car soit $\alpha = \bar{a}e^{ri}$, $\pi = re^{i\varphi}$ ou ($i = \sqrt{-1}$) les coordonnées polaires d'un point situé sur une droite satisfont à

$$r \cos(\delta - \varphi) = d,$$

où δ et d désignent l'inclinaison de la droite sur Ox, et d la distance de l'origine à la droite.

On a alors

$$\pi_1 = \mathrm{R}e^{i\Phi} = \bar{a}re^{\alpha + \varphi, i} \quad i = \sqrt{-1},$$

soit

$$\delta_1 = \delta + \alpha, \qquad d_1 = d\bar{a},$$

on voit que R et Φ satisfont à

$$R \cos (\delta_1 - \Phi) = d_1,$$

c'est-à-dire que tous les points δ_1 sont encore en ligne droite, car δ_1 et d_1 sont des constantes. Il en résulte de plus, que des droites parallèles qui correspondent à la même valeur de δ se transforment en droites parallèles correspondant à δ_1. La forme $\pi_1 = \bar{a}re^{i(\alpha + \varphi)}$ nous apprend que la multiplication par le nombre α, revient à faire tourner tout rayon vecteur parti de l'origine d'un angle $\hat{\alpha}$, et que ce vecteur est remplacé par un vecteur proportionnel, dans le rapport $\frac{\bar{a}r}{r} = \bar{a}$. Toute figure est donc transformée en une figure semblable.

L'idéal (α) s'obtient en multipliant par α l'idéal (1), le réseau (α) est donc un réseau semblable au réseau fondamental.

La maille du réseau fondamental de sommets 0, 1, $1 + \sqrt{-5}$, $\sqrt{-5}$ a pour homologue la maille de sommets 0, α, $\alpha + \alpha\sqrt{-5}$ et $\alpha\sqrt{-5}$.

Le rectangle qui est semblable à la maille du réseau fondamental, ne peut contenir d'autre point du réseau (α). D'où :

Théorème. — A tout idéal principal (α), déterminé par le nombre $\alpha = \bar{a}e^{i\alpha}$, correspond un réseau de points, semblable au réseau fondamental, et qui se déduit de celui-ci par une rotation d'angle $\hat{\alpha}$ et une homothétie, dont le rapport est $\bar{a} : 1$.

Il en résulte que les réseaux correspondants à tous les idéaux principaux sont semblables.

Au point de vue analytique, on voit que les points du réseau (α) résultent du réseau fondamental par une transformation homographique.

Soit $\alpha = a + b\sqrt{-5}$, et soit $x + y\sqrt{-5}$ un point du réseau fondamental, $X + Y\sqrt{-5}$ son homographique dans (α), on a

$$X = ax - 5by,$$
$$Y = bx + ay,$$

le déterminant de la transformation est $a^2 + 5b^2 = \bar{a}^2$. On peut inscrire une infinité de réseaux de parallèles dans le réseau (α), se déduisant l'un de l'autre par une transformation homographique de déterminant ± 1, comme il a été fait pour le réseau fondamental.

On peut attribuer à chaque base de l'idéal (α) un parallélogramme élémentaire ; par exemple, à α, $\alpha\sqrt{-5}$ nous attribuerons le parallélogramme dont les sommets sont o, $\alpha, \alpha\sqrt{-5}, \alpha + \alpha\sqrt{-5}$.

Aux différentes bases correspondent les différents réseaux de parallèles, et la façon dont on passe d'un couple de base à un autre, nous montre encore que ces réseaux s'obtiennent par des transformations homographiques. D'où :

Théorème. — On peut inscrire une infinité de réseaux de parallèles dans un réseau de points (α), chaque base de l'idéal définit un de ces réseaux de parallèles. Deux quelconques de ces réseaux sont homographiques, le déterminant de la transformation étant égal à $\pm$ 1, et la transformation elle-même est corrélative de celle qui relie les deux couples de nombres de base. Tous ces réseaux de parallèles ont des mailles de même aire.

Remarque : Lorsqu'on établit les formules de transformation qui permettent de passer d'un réseau de parallèles de (α) à un autre, on prend des axes obliques, parallèles aux droites de l'un des réseaux. On pourrait aussi rapporter ces formules aux axes de coordonnées rectangulaires primitifs. On aurait alors des formules de transformation, dont les coefficients seraient nécessairement rationnels, mais qui pourraient être fractionnaires, le déterminant serait toujours $\pm$ 1.

Ceci n'a pas d'importance, car le but poursuivi, seul détermine le choix des unités de longueur et les axes de coordonnées.

Toute maille d'un réseau contient, outre ses quatre sommets, un certain nombre d'autres points du réseau fondamental, à l'intérieur ou sur les côtés. Nous considérerons comme appartenant à une maille : 1. Un sommet de la maille (de telle sorte que tout sommet n'appartienne qu'à une seule maille) ; 2. Les points situés sur les côtés, se coupant au sommet, et qui ne sont pas des sommets ; 3. Les points situés à l'intérieur de la maille. Ceci posé, déterminons le nombre des points qui appartiennent à une maille (α) du réseau. Tout d'abord, on reconnaît que toutes les mailles d'un même réseau contiennent le même nombre de points du réseau fondamental. De plus, comme les mailles de deux réseaux différents s'obtiennent par une transformation homographique, qui a la propriété de faire correspondre à un point intérieur d'une maille, un point intérieur de l'autre, on voit que deux mailles, appartenant

à des réseaux différents, contiennent le même nombre de points entiers. Pour déterminer le nombre de ces points, prenons une maille quelconque ; choisissons celle qui appartient à la base normale.

Soit $\alpha = a + b\sqrt{-5}$, admettons que a et b aient t pour p. g. c. d., la base normale est $\frac{a^2 + 5b^2}{t}$, $a_1 + t\sqrt{-5}$, où a_1 est un multiple de t, cette maille a un de ses côtés situés sur Ox, elle contient $\frac{a^2 + 5b^2}{t}$ points du système fondamental, tandis que le côté déterminé par $a_1 + t\sqrt{-5}$ en contient t, et la maille contient en tout $n(\alpha) = a^2 + 5b^2$ points du réseau fondamental ; ces points forment un système complet de nombres incongrus, suivant le module (α).

Théorème. — Lorsqu'on inscrit un réseau de parallèles dans le réseau de points (α), chaque maille contient $n(\alpha)$, sommets du réseau fondamental, et ces sommets forment un système complet de nombres incongrus du corps, suivant le module (α).

Ce qui précède nous permet d'abréger ce qui va suivre.

Nous ferons correspondre à un idéal non principal

$$\mathfrak{j} = (\alpha, \beta, \gamma, \dots \lambda_1\alpha + \lambda_2\beta + \lambda_3\gamma, \dots),$$

le réseau des points α, β, γ, ... On peut représenter l'idéal $\mathfrak{j}$ par une base $(i_1, i_2, yi_1 + xi_2)$, où x, y parcourent tous les entiers rationnels de $-\infty$ à $+\infty$. Il en résulte que l'on peut inscrire dans le réseau de points $\mathfrak{j}$, un réseau de parallèles, dont la maille est déterminée par les points o, i_1, i_2, $i_1 + i_2$. A toute autre base de $\mathfrak{j}$ correspond un réseau de parallèles inscrit dans le réseau de points, et ces réseaux sont homographiques l'un de l'autre, les mailles de tous ces réseaux ayant même aire.

Le nombre des points du réseau fondamental, contenus à l'intérieur d'une maille d'un pareil réseau, est égal à la norme de l'idéal $n(\mathfrak{j})$, et les nombres représentés par ces points forment un système complet de nombres incongrus du corps, suivant le module $(\mathfrak{j})$.

Soient $\mathfrak{j}$ et $\mathfrak{j}_1$ deux idéaux non principaux de la même classe d'idéaux, comment les deux réseaux correspondants se déduisent-ils l'un de l'autre.

D'après la définition de l'équivalence, il y a deux nombres α et β, tels que

$$(\alpha)\mathfrak{j} = (\alpha_1)\mathfrak{j}_1.$$

Le produit $(\alpha)\mathfrak{j}$ n'est autre que l'idéal obtenu en multipliant tous les nombres de l'idéal $\mathfrak{j}$ par α. Si l'on remarque encore que α peut s'écrire $\alpha = \overline{a}e^{i\pi\hat{\alpha}}$, on voit que le réseau de points $\mathfrak{j}$ est transformé en un nouveau réseau de points $(\alpha)\mathfrak{j}$, qui se déduit du premier par une rotation α et par une homothétie $a : 1$, c'est-à-dire qu'à tout réseau inscrit dans $\mathfrak{j}$ correspond un réseau semblable inscrit dans $(\alpha)\mathfrak{j}$. De même le réseau $(\alpha_1)\mathfrak{j}_1$ résulte de $\mathfrak{j}_1$ par une similitude, c'est-à-dire que $\mathfrak{j}$ et $\mathfrak{j}_1$ sont semblables.

Nous pouvons donc énoncer :

Théorème. — Deux idéaux d'une même classe sont représentés géométriquement par des réseaux de points semblables. Deux réseaux de parallèles, inscrits dans ces réseaux, sont liés par une transformation homographique, dont le déterminant est

$$\pm\sqrt{n\left(\frac{\mathfrak{j}_1}{\mathfrak{j}}\right)}.$$

L'équivalence de deux idéaux, n'est autre chose que la similitude de leurs réseaux de points, ou des réseaux de parallèles qui y sont inscrits.

Le produit de deux idéaux $\mathfrak{j}$ et de $\mathfrak{j}_1$ est un idéal $\mathfrak{j}\mathfrak{j}_1$, que l'on peut considérer comme la résultante géométrique des deux réseaux de points $\mathfrak{j}$ et $\mathfrak{j}_1$. Le réseau $\mathfrak{j}\mathfrak{j}_1$ contient tous les points communs aux deux réseaux $\mathfrak{j}$ et $\mathfrak{j}_1$.

Lorsqu'on réunit tous les nombres de $\mathfrak{j}$ et $\mathfrak{j}_1$ pour former un nouvel idéal $\mathfrak{J}$, ce dernier est le plus grand commun diviseur idéal de $\mathfrak{j}$ et de $\mathfrak{j}_1$, on l'obtient géométriquement en superposant les deux réseaux $\mathfrak{j}$ et $\mathfrak{j}_1$.

Les théorèmes établis jusqu'ici sont tous valables pour $m \not\equiv 1\ (4)$. Dans le cas où $m \equiv 1\ (4)$, les entiers du corps sont $a + b\,\frac{1+\sqrt{m}}{2}$. Les points ou sommets du réseau fondamental sont formés par les points entiers d'un système de coordonnées obliques, que l'on choisit en sorte que l'origine des coordonnées soit au point zéro, et les points unités tombent aux points 1 et $\frac{1+\sqrt{m}}{2}$ situés sur les axes.

Parmi les réseaux de parallèles inscrits dans le réseau de points formés par les nombres entiers du corps, il n'y a pas de réseau dont la maille est un rectangle. On peut choisir comme maille d'un des réseaux un losange, c'est le losange

$$0, \frac{1+\sqrt{m}}{2}, \quad 1, \frac{1-\sqrt{m}}{2}.$$

Dans le réseau de points du corps $k(\sqrt{-3})$, les unités différentes de ± 1 ont une signification particulière, elles définissent les symétries de ce réseau, dont il sera parlé plus loin, à propos des corps réels. D'ailleurs tous les théorèmes démontrés plus haut s'appliquent exactement au cas du corps $m \equiv 1$ (4).

Le théorème arithmétique sur la limite finie de h, nombre des classes du corps $k(\sqrt{m})$, prend la forme géométrique suivante :

Théorème (1). — Les réseaux des points en nombre illimité, que l'on peut choisir dans le réseau des points du corps $k(\sqrt{m})$, en réunissant des sous-groupes de ce dernier, se répartissant en h groupes (ou classes), tels que tous les réseaux d'un même groupe (classe), ainsi que les réseaux de parallèles que l'on peut y inscrire soient semblables entre eux.

Les réseaux qui appartiennent à une même classe, et ceux-là seulement, forment des figures semblables. Un calcul direct montre que l'aire de la maille du réseau correspondant à l'idéal $\mathfrak{j}$ est égale à $\frac{1}{2} n(\mathfrak{j}) \sqrt{|d|}$ où $|d|$ est la valeur absolue du discriminant du corps.

Le théorème de Minkowski peut alors s'énoncer :

Théorème. — Dans chacun des h groupes de réseaux semblables du corps, il y en a au moins un dont la maille est $< \frac{|d|}{2}$.

Ce théorème nous donne un moyen de construire géométriquement les réseaux de points.

Quel est le réseau dont la maille est la plus simple, ce qui revient à dire, quelle est la base la plus simple d'un idéal : on peut considérer comme telle la base normale. On pourra alors en déduire

(1) Voir KLEIN, *l. c.*, t. II, p. [illegible]4.

que : dans tout réseau de maille $< \frac{|d|}{2}$ on peut inscrire un parallélogramme élémentaire dont les côtés sont $< \sqrt{|d|}$ respect. que

$$\sqrt{\frac{|d|}{2}}.$$

La représentation géométrique des imaginaires, et la correspondance si simple entre les opérations géométriques et les opérations arithmétiques, nous a permis de donner une interprétation géométrique très simple des résultats obtenus dans l'étude des corps imaginaires.

La raison de la simplicité tient de ce fait, que tout nombre complexe $a + b\sqrt{-1}$ peut être mis sous la forme

$$re^{\sqrt{-1}\varphi} = r(\cos\varphi + \sqrt{-1}\sin\varphi),$$

et qu'alors la multiplication de deux nombres complexes se ramène à la multiplication des modules r et r_1 et à l'addition des arguments φ et φ_1.

Soit un corps réel $k(\sqrt{m})$ [où nous supposerons tout d'abord $m \not\equiv 1$ (4)]. Nous pourrons encore former un réseau de points d'une manière analogue à la précédente.

Nous prendrons deux axes de coordonnées rectangulaires, nous mesurerons les abscisses avec une unité égale à 1 et les ordonnées avec une unité égale à $\sqrt{m}$, et à tout nombre $a + b\sqrt{m}$ nous ferons correspondre un point de coordonnées a et b. On a encore le théorème : un point du réseau $\pm$ un point du réseau est un point du réseau. La multiplication n'est plus définie.

De plus, si l'on représente un idéal par un réseau, il ne peut plus être question de la similitude des réseaux des idéaux principaux ou des réseaux appartenant à une même classe d'idéaux.

Nous allons mettre à profit une idée due à M. Klein (1), qui nous permettra d'établir l'accord entre les corps imaginaires et les corps réels. Nous remplacerons les notions élémentaires de mesure de longueurs et d'angles, qui est le système euclidien des mesures, par le système des mesures pseudomitriques.

---

(1) Klein, p. 50 et suiv., spécialement 71.

Nous allons insérer, dans la géométrie élémentaire, une série de définitions, de façon à obtenir un système géométrique sans contradictions.

Nous adopterons le système de coordonnées dont il vient d'être question, et nous définirons : 1. La distance de deux points ; 2. L'angle de deux droites ; 3. L'aire d'une figure fermée.

1. Soit x, $y\sqrt{m}$ ou (x, y) un point P du réseau et O le point (o — o),

$$r = +\sqrt{x^2 - my^2},$$

est par définition la distance $\overline{\text{OP}}$.

Tous les points, dont la distance à o est égale à 1, satisfont à

$$1 = x^2 - my^2,$$

ils sont situés sur une hyperbole réelle, dont l'axe réel est placé sur Ox, et dont la longueur est 2. Cette courbe est dite la *courbe mensurante* (*Eichkurve*), elle détermine l'unité de longueur. Elle définit, en effet, une unité de longueur (particulière) sur toute droite passant par l'origine, qui représente alors l'unité de mesure pour tout segment porté par la même droite.

Tous les points situés sur l'une des asymptotes

$$x - \sqrt{m}y = 0, \qquad x + \sqrt{m}y = 0,$$

sont situés à une distance de l'origine égale à o ; car, pour un point quelconque de l'une de ces asymptotes

$$r = \sqrt{x^2 - my^2} = 0.$$

Les asymptotes jouent, dans ce système, le rôle des droites $x \pm y\sqrt{-1}$ dans la géométrie élémentaire.

Cette propriété particulière a fait donner aux asymptotes le nom de droites minima, qui est employé en géométrie élémentaire pour

$$x + y\sqrt{-1} = 0 \qquad \text{et} \qquad x - y\sqrt{-1} = 0.$$

Les distances de tous les points situés à l'*intérieur* des asymptotes au point o sont réelles. Par contre, pour les autres points, $x^2 - my^2$ est négatif, par conséquent r est imaginaire. On peut utiliser pour ces points l'hyperbole conjuguée

$$x^2 - my^2 = -1,$$

comme courbe mensurante, à condition de multiplier l'unité obtenue par $i = \sqrt{-1}$.

De plus, la distance de deux points $x, y\sqrt{m}$, $x_1, y_1\sqrt{m}$ est

$$r = \sqrt{(x - x_1)^2 - m(y - y_1)^2}.$$

2. On emploie un artifice pour définir la pente du rayon OP. On remplace les fonctions circulaires employées précédemment par les fonctions hyperboliques, de même que pour les longueurs, l'hyperbole s'est substituée au cercle.

Nous poserons

$$x + y\sqrt{m} = r\,(\text{ch}\,\varphi + \text{sh}\,\varphi),$$

$$\left\{\begin{aligned} x &= r\,\text{ch}\,\varphi, \\ y\sqrt{m} &= r\,\text{sh}\,\varphi, \end{aligned}\right.$$

et cet angle φ, qui par définition sera l'angle de OP avec Ox.

Rappelons ici les propriétés élémentaires des fonctions hyperboliques,

$$\text{ch}\,\varphi = \frac{e^{\varphi} + e^{-\varphi}}{2}, \qquad \text{sh}\,\varphi = \frac{e^{\varphi} - e^{-\varphi}}{2},$$

par suite

$$\text{ch}\,(-\varphi) = \text{ch}\,(\varphi), \qquad \text{sh}\,(-\varphi) = -\,\text{sh}\,\varphi,$$

$$\text{ch}^2\,\varphi - \text{sh}^2\,\varphi = 1, \qquad \text{donc} \qquad x^2 - my^2 = r^2,$$

de plus

$$\text{ch}\,\varphi - \text{sh}\,\varphi = e^{\varphi}, \qquad \text{ch}\,\varphi - \text{sh}\,\varphi = e^{-\varphi}.$$

$$(\text{ch}\,\varphi + \text{sh}\,\varphi)\,(\text{ch}\,\varphi_1 + \text{sh}\,\varphi_1) = \text{ch}\,(\varphi + \varphi_1) + \text{sh}\,(\varphi + \varphi_1),$$

$$(\text{ch}\,\varphi + \text{sh}\,\varphi)\,(\text{ch}\,\varphi_1 - \text{sh}\,\varphi_1) = \text{ch}\,(\varphi - \varphi_1) + \text{sh}\,(\varphi - \varphi_1),$$

$$(\text{ch}\,\varphi - \text{sh}\,\varphi)\,(\text{ch}\,\varphi_1 - \text{sh}\,\varphi_1) = \text{ch}\,(\varphi + \varphi_1) - \text{sh}\,(\varphi + \varphi_1),$$

$$(\text{ch}\,\varphi + \text{sh}\,\varphi) : (\text{ch}\,\varphi_1 + \text{sh}\,\varphi_1) = \text{ch}\,(\varphi - \varphi_1) + \text{sh}\,(\varphi - \varphi_1),$$

$$(\text{ch}\,\varphi + \text{sh}\,\varphi) : (\text{ch}\,\varphi_1 - \text{sh}\,\varphi_1) = \text{ch}\,(\varphi + \varphi_1) + \text{sh}\,(\varphi - \varphi_1),$$

$$(\text{ch}\,\varphi - \text{sh}\,\varphi) : (\text{ch}\,\varphi_1 - \text{sh}\,\varphi_1) = \text{ch}\,(\varphi - \varphi_1) - \text{sh}\,(\varphi - \varphi_1).$$

D'après cette formule, l'analogie de la multiplication de deux nombres

$$x + y\sqrt{m} = r\,(\text{ch}\,\varphi + \text{sh}\,\varphi) \quad \text{et} \quad x_1 + y_1\sqrt{m} = r_1\,(\text{ch}\,\varphi_1 + \text{sh}\,\varphi_1),$$

avec la multiplication des nombres complexes est complète.

Lorsqu'on veut déterminer φ on a

$$x + y\sqrt{m} = re^{\varphi},$$

$$x - y\sqrt{m} = re^{-\varphi},$$

$$e^{2\varphi} = \frac{x + y\sqrt{m}}{x - y\sqrt{m}},$$

$$\varphi = \frac{1}{2}\,\mathrm{L}\,\frac{x + y\sqrt{m}}{x - y\sqrt{m}}.$$

Mais comme $e^{2\varphi} = e^{2\varphi + 2\pi i}$, on voit que φ n'est déterminé qu'au module πi près. Nous entendrons par Log la valeur principale (réelle) du Logarithme naturel du quotient $\frac{x + y\sqrt{m}}{x - y\sqrt{m}}$. Il faut alors distinguer entre les rayons OP qui coupent l'hyperbole $x^2 - my^2 = 1$, et ceux qui ne la coupent pas.

Dans le premier cas $x^2 - my^2 > 0$, ou encore la norme du nombre $x + y\sqrt{m}$ est positive, r est réel, alors

$$\varphi = \frac{1}{2}\,\mathrm{L}\,\frac{x + y\sqrt{m}}{x - y\sqrt{m}} = \frac{1}{2}\,\mathrm{L}\,\frac{(x + y\sqrt{m})^2}{n(x - y\sqrt{m})},$$

φ est un angle réel.

Dans le second cas $x^2 - my^2 < 0$, $n(x + y\sqrt{m})$ est négatif,

$$\varphi = \frac{1}{2}\,\mathrm{L}\,\frac{(x + y\sqrt{m})^2}{n(x - y\sqrt{m})} = \frac{1}{2}\,\mathrm{L}\left[-\frac{(x + y\sqrt{m})^2}{n(x - y\sqrt{m})}\right] + \frac{1}{2}\,\mathrm{L}\,(-1),$$

$$\varphi = |\varphi| = \frac{1}{2}\,i\pi.$$

L'angle φ est un nombre complexe.

L'angle de deux rayons OP, OP_1 est, par définition, la différence des pentes de ces rayons $\varphi - \varphi_1$, précédé du signe + ou —. Le signe sera déterminé lorsqu'on aura orienté les angles. Deux rayons vecteurs, séparés par une asymptote, comprennent un angle complexe, tandis que deux rayons qui ne sont pas séparés par une asymptote comprennent un angle réel. L'angle d'une asymptote avec Ox ou avec un rayon quelconque OP est infiniment grand.

3. Nous prendrons pour unité de surface un carré de côté égal à 1. Nous mesurerons les aires suivant les procédés habituels de la géométrie élémentaire, c'est-à-dire du calcul intégral.

La surface d'un parallélogramme de sommets o, $a + b\sqrt{m}$, $a + a_1 + (b + b_1)\sqrt{m}$, $a_1 + b_1\sqrt{m}$, est égale à

$$f = \begin{vmatrix} a & b\sqrt{m} \\ a_1 & b_1\sqrt{m} \end{vmatrix} = (ab_1 - a_1b)\sqrt{m},$$

et, en particulier, la maille du réseau des nombres entiers du corps du réseau fondamental, a une aire égale à $\sqrt{m}$.

Il est évident, d'après ces conventions, que les théorèmes fondamentaux relatifs aux opérations élémentaires de l'addition, de la soustraction, de la multiplication sont encore vrais. La multiplication de deux sommets du réseau, revient à l'addition des pentes de leurs rayons vecteurs et à la multiplication de ces rayons vecteurs r et r_1.

Un idéal principal (α) est donc représenté par un réseau de points, composé de tous les points du réseau divisibles par α. La représentation de l'idéal (α) par une base quelconque, par exemple α, $\alpha\sqrt{m}$,

$$(\alpha) = (\alpha, \alpha\sqrt{m}, \alpha x + \alpha\sqrt{m}y),$$

où x et y sont des entiers rationnels, nous montre que l'on peut inscrire une infinité de réseaux de parallèles dans le réseau de l'idéal.

On obtient le réseau (α) en multipliant tout point du réseau fondamental par α. Soit $\alpha = a + b\sqrt{m} = \overline{a}e^{\hat{\alpha}}$ et soit $x + y\sqrt{m} = re^{\varphi}$ un point quelconque du réseau, on a comme produit de ces deux points

$$X + Y\sqrt{m} = ax + bmy + (bx + ay)\sqrt{m} = \overline{a}re^{\hat{\alpha} + \varphi},$$

d'où le théorème :

Tout point de (α) résulte d'un point du réseau fondamental, par une rotation du rayon vecteur d'un angle $\hat{\alpha}$, et par une homothétie dans le rapport $\overline{a}$: 1.

On peut encore dire :

Le réseau (α) est lié au réseau des points du corps par la transformation

$$\begin{cases} X = ax + bmy, \\ Y = bx + ay, \end{cases}$$

dont le déterminant est $a^2 - mb^2 = \overline{a}^2$.

Nous venons d'employer le mot de « rotation » dans un sens un peu plus général que le sens ordinaire. Nous y sommes amenés, car cette rotation est contenue dans une transformation homographique et ces transformations sont essentiellement distinctes suivant que le déterminant de la transformation est positif ou négatif. En effet si $\overline{a}^2$ est positif notre angle

$$\hat{\alpha} = \frac{1}{2} \operatorname{Log} \frac{(a + b\sqrt{m})^2}{\overline{a}^2}$$

est réel et nous avons une rotation usuelle.

Si $\overline{a}^2$ est négatif, c'est-à-dire $\overline{a}$ imaginaire,

$$\hat{\alpha} = \frac{1}{2} i\pi + \frac{1}{2} \operatorname{L} \left[\frac{(a + b\sqrt{m})^2}{\overline{a}^2} \right]$$

est un angle complexe, et entre les deux positions du rayon vecteur il y a une asymptote. On peut considérer cette rotation impropre comme une combinaison d'une rotation de l'angle réel

$$\frac{1}{2} \operatorname{L} \left[- \frac{(a + b\sqrt{m})^2}{\overline{a}^2} \right]$$

où le rayon ne sort pas d'un angle des asymptotes, et d'une symétrie par rapport aux asymptotes.

[Trouver un rayon OP_1 qui fait avec OP l'angle $\frac{\pi i}{2}$ c'est trouver le rayon du faisceau de sommet O conjugué harmonique de OP par rapport aux asymptotes].

Prenons un exemple : le corps $k(\sqrt{10})$.

Les points $O = 0$, $\mathfrak{a} = 1$, $\mathfrak{b} = 1 + \sqrt{10}$, $\mathfrak{c} = \sqrt{10}$ nous donnent dans le réseau $(\alpha) = (1 + \sqrt{10})$ les quatre points

$$O = 0, \quad \mathfrak{A} = 1 + \sqrt{10}, \quad \mathfrak{B} = 11 + 2\sqrt{10}, \quad \mathfrak{C} = 10 + \sqrt{10}.$$

Les formules nous donnent

$$\varphi_{\mathfrak{a}} = \frac{1}{2} \operatorname{L} \frac{1 + \sqrt{10}}{1 - \sqrt{10}},$$

$$\varphi_{\mathfrak{b}} = \frac{1}{2} \operatorname{L} \frac{11 + 2\sqrt{10}}{11 - 2\sqrt{10}},$$

$$\varphi_{\mathfrak{c}} = \frac{1}{2} \operatorname{L} \frac{10 + \sqrt{10}}{10 - \sqrt{10}}.$$

et enfin

$$\mathfrak{A}O\mathfrak{C} = \frac{1}{2}\,\mathrm{L}\,(-1) = \sphericalangle\,\mathfrak{a}O\mathfrak{c}.$$

On voit de même que les angles

$$O\mathfrak{A}\mathfrak{B} = O\mathfrak{a}\mathfrak{b}, \quad \mathfrak{A}\mathfrak{B}\mathfrak{C} = \mathfrak{a}\mathfrak{b}\mathfrak{c}, \quad \mathfrak{B}\mathfrak{C}O = \mathfrak{b}\mathfrak{c}O.$$

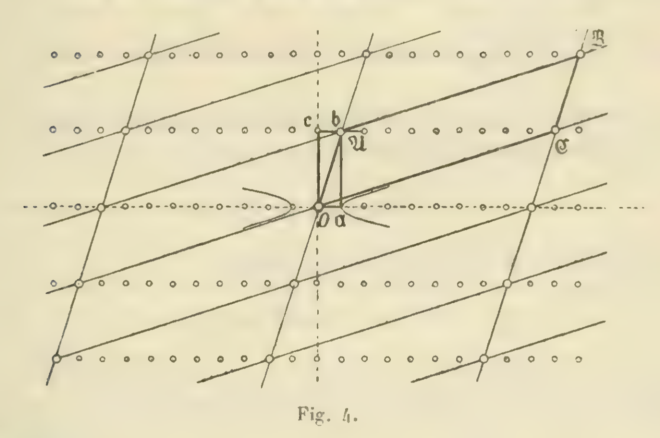


Fig. 4.

De plus

$$O\mathfrak{A} : O\mathfrak{C} = \sqrt{-9} : \sqrt{90} = \sqrt{-1} : \sqrt{10},$$
$$O\mathfrak{a} : O\mathfrak{c} = 1 : \sqrt{-10} = O\mathfrak{A} : O\mathfrak{C},$$

et l'on voit qu'aux sens des conventions pseudométriques les figures $O\mathfrak{a}\mathfrak{b}\mathfrak{c}$ et $O\mathfrak{A}\mathfrak{B}\mathfrak{C}$ sont semblables.

On a donc le résultat suivant :

Le réseau (α) est semblable au réseau fondamental et résulte de ce dernier par une rotation $\widehat{\alpha} = \frac{1}{2}\,\mathrm{L}\,\frac{a + b\sqrt{m}}{a - b\sqrt{m}}$ et une homothétie de rapport $\overline{a} : 1$.

On démontre exactement comme dans le cas des corps imaginaires que l'on peut inscrire une infinité de réseaux de parallèles dans un réseau de points (α) et que deux de ces réseaux se déduisent l'un de l'autre par une transformation homographique de déterminant ± 1.

Il nous reste pour bien connaitre la structure d'un réseau (α) à chercher la signification géométrique des idéaux unités.

Il a été démontré précédemment qu'un corps réel possède une

infinité d'unités. Leurs images sont situées sur la courbe mensurante (Eichkurve). L'image de l'unité fondamentale est parmi ces points celui qui a la moindre pente.

Soit ε une unité du corps de norme $n(\varepsilon) = + 1$.

Le réseau (ε) comprend tous les points du corps. Le réseau (ε) s'obtient en donnant au réseau du corps une rotation

$$\hat{\varepsilon} = \frac{1}{2} \mathrm{L} \frac{a + b\sqrt{m}}{a - b\sqrt{m}} = \mathrm{L}(a + b\sqrt{m}) \qquad \text{car} \qquad \bar{e} = n(\varepsilon) = + 1.$$

De même le réseau (ε^k) où k est un entier positif ou négatif s'obtient en donnant au réseau du corps la rotation

$$k\,\mathrm{L}(a + b\sqrt{m}),$$

et le réseau $(-\varepsilon^k)$ s'obtient par la rotation

$$k\,\mathrm{L}(a + b\sqrt{m}) + i\pi.$$

Mais comme tous ces réseaux $(\pm \varepsilon^k)$ sont identiques au réseau fondamental on voit qu'on peut donner à l'existence des unités du corps en nombre infini l'interprétation géométrique suivante :

Le réseau des points entiers du corps $k(\sqrt{m})$ se transforme en lui-même par une rotation d'un multiple quelconque de $\hat{\varepsilon}$, c'est-à-dire $k\hat{\varepsilon}$ ou encore $i\pi + k\hat{\varepsilon}$. Dans ces rotations les points unités se déplacent sur la Eichkurve et un point quelconque se déplace sur une hyperbole $x^2 - my^2 = \mathrm{C}$ semblable à une Eichkurve (propre ou impropre).

Le réseau de points d'un corps réel a donc des propriétés analogues à celles d'un polygone régulier ou plutôt à celle d'un polygône inscrit dans un cercle et admettant certaines symétries.

Soit ensuite une unité ε de $k(\sqrt{m})$ dont la norme égale à -1, il est encore vrai que le réseau (ε) est identique au réseau du corps. Il se déduit du premier par une rotation impropre

$$\hat{\varepsilon} = \frac{1}{2} \mathrm{L} \frac{a + b\sqrt{m}}{a - b\sqrt{m}} = \mathrm{L}(a - b\sqrt{m}) - \frac{1}{2} \mathrm{L}(-1)$$

$$= -\frac{1}{2} i\pi + \mathrm{L}(a + b\sqrt{m}),$$

c'est-à-dire par une rotation compliquée d'une symétrie par rapport

aux asymptotes, avec une transformation du rayon vecteur dans le rapport $i : 1$.

Le réseau $(-\varepsilon)$ ne diffère du réseau (ε) que par une symétrie par rapport au point O.

Le réseau (ε^2) résulte du réseau fondamental par une rotation propre. ε^{2k+1} se distingue donc de ε^{2k}, du reste on peut énoncer général le :

Théorème. — Lorsque le corps réel renferme une unité fondamentale ε de norme -1 et si l'on pose $\varepsilon = ie^{\frac{i\pi}{2} + \varepsilon_1}$ où ε_1 est un angle réel, le réseau se transforme en lui-même par une rotation d'un angle $\hat{\varepsilon}_1$ suivie d'une symétrie par rapport à une asymptote de la courbe mensurante (Eichkurve).

Ces deux interprétations géométriques expliquent les théorèmes relatifs aux unités du corps quadratique et montrent l'intérêt de la différence entre la norme positive et la norme négative de l'unité fondamentale.

Connaître les unités du corps réel ce n'est au point de vue analytique que connaître toutes les transformations linéaires à coefficients entiers

$$X = ax + bmy,$$
$$Y = bx + ay,$$

qui transforme en lui-même le réseau du corps, car il est évident qu'une pareille transformation ne peut avoir comme déterminant que ± 1.

Pour les corps imaginaires à l'exception peut-être de $k(\sqrt{-3})$ la recherche de ces transformations est un problème facile.

Le corps $k(\sqrt{-1})$ nous donne un réseau fondamental contenant un réseau de parallèles à mailles carrées. Ce réseau se transforme en lui-même par une rotation de 90° et par une symétrie par rapport aux bissectrices des angles des axes. L'interprétation géométrique des unités $\pm\sqrt{-1}$ donnerait le même résultat.

Il est de plus évident que les unités jouent le même rôle pour un réseau de points (α) que pour le réseau des nombres du corps car $(\alpha) = (\alpha\varepsilon)$, c'est-à-dire les unités fournissent toutes les rotations (propres et impropres) ou au point de vue analytique toutes les transformations qui font coïncider un réseau (α) avec lui-même.

Nous avons examiné tous les cas où les résultats diffèrent pour les corps réels et les corps imaginaires. Il est facile de compléter pour les cas où les interprétations sont semblables dans les deux espèces de corps. Nous négligerons de traiter le cas d'un corps réel $m \equiv 1$ (4) et nous contenterons d'énoncer le résultat final.

Théorème. — Lorsqu'on attribue aux entiers d'un corps un réseau de points, à tout idéal j du corps correspond un réseau de points j. On peut inscrire une infinité de réseau de parallèles dans ce dernier. Ils se déduisent l'un de l'autre par une transformation homographique de déterminant ± 1. Tout réseau de points se transforme en lui-même d'une infinité de manières. Ces transformations sont fournies par les unités du corps.

La maille d'un réseau contient des sommets du réseau fondamental formant un système complet de restes suivant j).

Les réseaux correspondant à des idéaux équivalents sont semblables, de sorte que l'ensemble des réseaux de points se répartissent en h classes. Chaque classe contient au moins un réseau avec une maille d'aire $< \frac{d}{2}$.

CHAPITRE IV

—

LES CORPS DU TROISIÈME DEGRÉ

Nous avons traité assez complètement la théorie des corps quadratiques dans les chapitres précédents. Notre intention était de familiariser le lecteur avec les problèmes de la théorie d'un corps quelconque. Le corps quadratique cependant est si particulier que le plus souvent il ne faut pas appliquer à son étude les méthodes de la théorie générale des corps algébriques. On pourrait encourir le reproche d'employer des canons pour tuer des moineaux.

Ce livre se propose de servir d'introduction à l'étude des corps algébriques, et pour atteindre notre but nous ajouterons encore quelques méthodes plus générales sur lesquelles se base la théorie des idéaux. C'est pourquoi nous étudierons le corps cubique à l'exception : 1° des lois de réciprocité ; 2° de la répartition des classes en genres.

Nous ne donnerons d'une façon complète que les démonstrations qui diffèrent essentiellement des démonstrations pour les théorèmes correspondants du corps quadratique.

Enfin le dernier chapitre est destiné à expliquer une notion extrêmement importante et fructueuse, celle du « corps relatif », nous l'expliquerons sur l'exemple d'un corps relatif par rapport au corps quadratique pris comme corps fondamental.

39. Notions fondamentales. Définitions. — Tout nombre α racine d'une équation irréductible de degré m à coefficients rationnels est dit un nombre algébrique.

Si l'on adjoint ce nombre α aux nombres rationnels, et si l'on effectue sur ce système de nombres étendu ainsi les opérations d'addition, de soustraction, de multiplication et de division, on obtient un nouveau *domaine* de nombres algébriques ou un *corps de nombres*. Autrement dit ce corps se compose de toutes les fonctions rationnelles entières et fractionnaires de α à coefficients rationnels. Le corps de nombres a les propriétés fondamentales suivantes qui peuvent être prises pour définition :

1° La somme ou la différence de deux nombres est un nombre du corps ;

2° Le produit et le quotient de deux nombres quelconques est un nombre du corps.

Un nombre algébrique α est dit un nombre algébrique *entier* lorsque α satisfait à une équation algébrique de degré m

$$\alpha^m + a_1\alpha^{m-1} + \dots + a_m = 0,$$

où $a_1, a_2, \dots a_m$ sont des entiers rationnels, tandis que le coefficient de α^m égale 1.

Nous nous occuperons de suite du corps du troisième degré (au corps cubique). Nous appliquerons ici certains théorèmes et certaines notations empruntés à l'algèbre, les traités d'algèbre renseigneront le lecteur à ce sujet.

Soient ϑ, ϑ', ϑ'' les racines d'une équation du troisième degré irréductible

$$G(x) = x^3 + a_1x^2 + a_2x + a_3 = 0$$

à coefficients entiers et rationnels a_1, a_2, a_3 ; ϑ, ϑ', ϑ'' sont trois *nombres algébriques distincts entiers* que nous ne supposerons pas rationnels.

Nous dirons que les trois nombres ϑ, ϑ', ϑ'' sont conjugués. En les adjoignant successivement au domaine des nombres rationnels on obtient trois corps de nombres différents que l'on nomme *corps conjugués*, nous les désignerons par $k(\vartheta)$, $k(\vartheta')$, $k(\vartheta'')$. $k(\vartheta')$ résulte de $k(\vartheta)$ quand on remplace dans tous les nombres de ce dernier ϑ par ϑ', ou encore lorsqu'on effectue la substitution $S = S(\vartheta : \vartheta')$.

Théorème. — Les nombres du corps $k(\vartheta)$ peuvent être représentés sous la forme

$$\theta = a + b\vartheta + c\vartheta^2,$$

a, b, c étant des nombres rationnels quelconques.

θ peut par définition s'écrire

$$\theta = \frac{f(\vartheta)}{f_1(\vartheta)},$$

où f, f_1 sont des fonctions rationnelles entières de degrés quelconques r et r_1 et à coefficients rationnels entiers. Les nombres $f(\vartheta)$, $f_1(\vartheta)$ sont $\neq 0$ par hypothèse. Les deux fonctions f et f_1 sont premières avec $G(x)$ (c'est-à-dire qu'elles ne peuvent avoir avec $G(x)$ aucun facteur commun de la forme $G_1(x) = b_0x^2 + b_1x + b_2$). Car comme $G(x)$ est une fonction irréductible $f(x)$ ou $f_1(x)$ serait divisible par $G(x)$ lui-même et on aurait $f(\vartheta) = 0$ ou $f_1(\vartheta) = 0$.

On sait qu'on peut déterminer deux polynômes rationnels $f_2(x)$, $G_2(x)$ à coefficients entiers rationnels et de degrés respectifs 2 et $r_1 - 1$, tels que

$$f_2(x) \cdot f_1(x) + G_2(x) G(x) = 1.$$

En tenant compte de $G(\theta) = 0$, on a

$$\theta = \frac{f(\vartheta)}{f_1(\vartheta)} = \frac{f_2(\vartheta) f(\vartheta)}{f_2(\vartheta) f_1(\vartheta) + G_2(\vartheta) G(\vartheta)} = f_2(\vartheta) f(\vartheta) = F(\vartheta),$$

c'est-à-dire qu'on voit tout d'abord que tout nombre du corps peut être représenté par un polynôme entier à coefficients rationnels. Mais tout polynôme de degré supérieur à 2 peut être mis sous la forme

$$F(x) = F_1(x) \cdot G(x) + G_1(x),$$

où $G_1(x)$ représente un polynôme du second degré au plus à coefficients rationnels, et comme $G(\vartheta) = 0$, $F(\vartheta) = G_1(\vartheta)$, c'est-à-dire que

$$\theta = a + b\vartheta + c\vartheta^2$$

est la forme la plus générale des nombres de $k(\vartheta)$ [1].

De là résulte que tout nombre θ non rationnel satisfait à une équation du troisième degré à coefficients rationnels.

---

[1] Comme $\vartheta' + \vartheta''$ et $\vartheta'\vartheta''$ sont des nombres du corps $k(\vartheta)$, il est facile de voir que $\theta' + \theta''$ et $\theta'\theta''$ sont comme θ des nombres du corps.

Cette proposition se démontre facilement, et nous passons de suite à l'étude des *entiers* du corps.

Théorème. — La somme, la différence, le produit de deux nombres entiers du corps $k(\vartheta)$ est un entier du corps.

Démonstration : Soient α et β deux nombres entiers du corps

$$\alpha = u + v\vartheta + w\vartheta^2,$$
$$\beta = u_1 + v_1\vartheta + w_1\vartheta^2,$$

où u, v, w, u_1, v_1, w_1 sont des nombres rationnels. ϑ, α, β satisfont à

$$(1) \qquad G(x) = x^3 + a_1x^2 + a_2x + a_3 = 0,$$
$$(2) \qquad x^3 + A_1x^2 + A_2x + A_3 = 0,$$
$$(3) \qquad x^3 + B_1x^2 + B_2x + B_3 = 0.$$

Il est évident tout d'abord que la somme $\alpha + \beta$ satisfait à une équation du troisième degré à coefficients rationnels, car les coefficients de

$$(4) \quad S(x) = [x - (\alpha + \beta)]\,[x - (\alpha' + \beta')]\,[x - (\alpha'' + \beta'')] = 0$$

peuvent être exprimés par des fonctions entières et rationnelles de u, v, w, u', v', w' et par des fonctions symétriques élémentaires de ϑ, ϑ', ϑ'', c'est-à-dire a_1, a_2, a_3. Le coefficient de x^3 est égal à 1. Il reste à démontrer que les autres coefficients sont des *entiers* rationnels.

Pour cela formons d'abord l'équation du neuvième degré

$$(5) \quad \begin{aligned} T(x) = [x - (\alpha + \beta)]\,[x - (\alpha + \beta')]\,[x - (\alpha + \beta'')] \dots \\ [x - (\alpha'' + \beta)]\,[x - (\alpha'' + \beta')]\,[x - (\alpha'' + \beta'')] = 0. \end{aligned}$$

Dans l'expression $T(x)$ le coefficient du terme de degré le plus élévé est 1, tous les autres coefficients sont des fonctions symétriques entières rationnelles de α, α', α'', β, β', β'', elles s'expriment rationnellement et en fonction entière des coefficients de (2) et de (3), c'est-à-dire des entiers rationnels A et B, c'est-à-dire que les coefficients de $T(x)$ sont des entiers rationnels, ceci démontrerait déjà que $\alpha + \beta$ est entier. On peut en conclure de plus ce qui suit :

La fonction $S(x)$ est un diviseur de $T(x)$, c'est-à-dire que $T(x)$ est le produit de deux fonctions entières rationnelles

$$T(x) = S(x)\, S_1(x).$$

Les coefficients de T et de S étant rationnels, ceux de S_1 le sont aussi, et le coefficient du premier terme de $S_1(x)$ est l'unité. D'après un théorème dû à Gauss [1] il en résulte que tous les coefficients de $S(x)$ et $S_1(x)$ sont des entiers rationnels, car il en est ainsi des coefficients de $T(x)$.

Le Théorème est donc démontré pour la somme et la différence. Lorsqu'il s'agit du produit, on remplace les opérations (4) et (5) par

$$(4a) \qquad Px = (x - \alpha\beta)(x - \alpha'\beta')(x - \alpha''\beta'') = 0.$$

$$(5a) \quad \left| \begin{array}{l} Q(x) = (x - \alpha\beta)(x - \alpha\beta')(x - \alpha\beta'')(x - \alpha'\beta)(x - \alpha'\beta')(x - \alpha'\beta'') \\ \qquad (x - \alpha''\beta)(x - \alpha''\beta')(x - \alpha''\beta''). \end{array} \right.$$

On achève comme précédemment.

On démontre ensuite de proche en proche le

Théorème. — Toute fonction rationnelle entière de nombres entiers du corps à coefficients entiers rationnels est encore un nombre entier du corps.

Une conséquence importante est la suivante :

Si α est un nombre entier $\alpha'\alpha''$ est aussi un entier, car $\alpha'\alpha'' = \frac{\alpha\alpha'\alpha''}{\alpha}$ est un nombre entier et que $\frac{\alpha\alpha'\alpha''}{\alpha}$ est un nombre du corps $k(\vartheta)$.

---

(1) Voir WEBER, *Traité d'algèbre*, 2e édition, Braunschweig, t. I, p. 98. Soient

$$\varphi(x) = x^m + a_1 x^{m-1} + \dots a_m$$
$$\psi(x) = x^n + b_1 x^{n-1} + \dots b_n$$

deux fonctions entières rationnelles, dont les premiers termes ont pour coefficient 1 ; tandis que les autres coefficients sont rationnels, les coefficients du produit

$$\varphi(x)\psi(x) = x^{m+n} + c_1 x^{m+n-1} + \dots + c_{m+n},$$

$c_1, c_2, c_3, \dots c_{m+n}$ ne peuvent être tous entiers que si les coefficients a, b de $\varphi(x)$ et de $\psi(x)$ sont tous des nombres entiers.

Nous appliquerons plus loin le

Théorème. — Lorsqu'un entier du corps $k(\zeta)$ est un nombre rationnel il est en même temps un entier rationnel.

La démonstration résulte du théorème de Gauss, si l'on considère que l'équation du troisième degré à laquelle satisfait α se décompose.

40. Le discriminant d'un nombre entier du corps. — Soit α un entier quelconque du corps.

1. Les nombres α', α'' issus de α en remplaçant ζ par ζ' et ζ'' sont dits *conjugués* de α.

2. Le produit

$$\alpha\alpha'\alpha'' = n(\alpha)$$

est la *norme* du nombre α.

3. Le produit

$$\delta(\alpha) = (\alpha - \alpha')(\alpha - \alpha'')$$

est la différente de α.

4. Le produit

$$d(\alpha) = (\alpha - \alpha')^2(\alpha - \alpha'')^2(\alpha' - \alpha'')^2 = \begin{vmatrix} 1 & \alpha & \alpha^2 \\ 1 & \alpha' & \alpha'^2 \\ 1 & \alpha'' & \alpha''^2 \end{vmatrix}^2$$

est le *discriminant* du nombre α.

La norme et le discriminant d'un nombre entier α sont des entiers rationnels, ils appartiennent au corps, la différente de α est aussi un nombre du corps, car

$$\delta(\alpha) = \alpha^2 - \alpha(\alpha' + \alpha'') + \alpha'\alpha'',$$

de plus on voit que

$$d(\alpha) = -n(\delta(\alpha)).$$

Le discriminant du nombre ζ qui détermine le corps $k(\zeta)$ est comme on sait une fonction rationnelle de a_1, a_2, a_3. Cette fonction ne peut être nulle car $G(x) = 0$ étant irréductible n'a pas de racine double.

L'algèbre nous apprend à calculer $d(\alpha)$ au moyen des fonctions symétriques. Pour $\mathfrak{z}$ qui est une racine de $G(x) = 0$, il vient

$$d(\mathfrak{z}) = a_1^2 a_2^2 + 18 a_1 a_2 a_3 - 4a_2^3 - 4a_1^3 a_3 - 27 a_3^2.$$

En particulier si $a_1 = 0$, on a

$$d(\mathfrak{z}) = -4a_2^3 - 27 a_3^2.$$

Le discriminant d'un nombre rationnel est évidemment égal à zéro. Réciproquement si le déterminant de α est nul α est un nombre rationnel. En effet si $d(\alpha) = 0$, $\alpha = \alpha'$, α est donc racine double d'une équation du troisième degré à coefficients rationnels, c'est-à-dire que α est rationnel. Tout nombre non rationnel α est racine d'une équation irréductible du 3[e] degré.

Dans le cas où $d(\mathfrak{z})$ est positif l'équation $G(x) = 0$ a trois racines réelles ; les trois corps conjugués $k(\mathfrak{z})$, $k(\mathfrak{z}')$, $k(\mathfrak{z}'')$ ne contiennent que des nombres réels, nous dirons que ce sont des corps réels.

Dans le cas où le discriminant $d(\mathfrak{z})$ est négatif l'équation $G(x) = 0$ a une racine réelle et deux racines imaginaires conjuguées. L'un des trois corps est un corps réel. Les deux autres contiennent des nombres imaginaires et sont dits des corps imaginaires.

Théorème. — Le discriminant de tout entier non rationnel d'un corps cubique est toujours différent de zéro et de ± 1.

Démonstration : Les discriminants de tous les nombres différents de zéro entiers et non rationnels ont le même signe. Car

$$\alpha = a_1 + b_1\mathfrak{z} + c_1\mathfrak{z}^2$$
$$\alpha^2 = a_2 + b_2\mathfrak{z} + c_2\mathfrak{z}^2$$

est d'après le théorème relatif au produit des déterminants

$$d(\alpha) = (b_1 c_2 - b_2 c_1)^2 d(\mathfrak{z}).$$

Le discriminant de tout nombre α a le signe du discriminant de $\mathfrak{z}$.

De plus α satisfait à une équation irréductible du troisième degré

$$(1) \qquad x^3 + u_1 x^2 + u_2 x + u_3 = 0$$

à coefficients entiers et rationnels. Ou bien $u_1 = 0$ et l'on a

$$d(\alpha) = -4u_2^3 - 27u_3^2,$$

ou bien u_1 est différent de zéro et la substitution

$$y = x + \frac{u_1}{3} \quad \text{ou} \quad x = y - \frac{u_1}{3}$$

ramène l'équation (1) à la forme

$$(2) \qquad y^3 + \frac{U_2}{3} y + \frac{U_3}{27} = 0,$$

où U_2, U_3 sont des entiers rationnels où U_2 est divisible par 3 et U_3 est divisible par 27 si u_1 est divisible par 3. S'il en est ainsi $d(\alpha)$ est de la forme $-4u_2'^3 - 27u_3'^2$.

Dans le cas où $u_1 \not\equiv 0 \ (3)$, on a

$$d(\alpha) = -4\frac{U_2^3}{27} - 27\frac{U_3^2}{27^2} = -\frac{1}{27}(4U_2^3 + U_3^2).$$

Si donc le discriminant d'un nombre entier était égal à -1, l'une des deux équations

$$(3) \qquad 4u_2^3 + 27u_3^2 = 1$$

$$(4) \qquad 4U_2^3 + U_3^2 = 27$$

aurait des solutions entières, c'est-à-dire que l'une des deux congruences

$$27u_3^2 - 1 \equiv 0 \ (4), \qquad U_3^2 - 27 \equiv 0 \ (4)$$

admettrait des solutions ce qui est impossible.

On ne peut avoir non plus $d(\alpha) = +1$. En effet, en cherchant à résoudre $x^3 + y^3 = z^3$, nous avons vu que les équations

$$(5) \qquad y^3 - y \pm \frac{1}{3} = 0$$

sont les seules équations à coefficients rationnels dont la somme est nulle et dont le discriminant $d(\alpha) = +1$. Ces équations ne définissent aucun nombre entier rationnel. Il n'y a pas non plus de substitution $y = x + \frac{u_1}{3}$ qui permet de déduire de (5) une équation

$$x^3 + u_1x^2 + u_2x + u_3 = 0$$

à coefficients entiers et rationnels comme on le voit en remplaçant y par sa valeur dans (5).

41. Les bases du corps $k(\mathfrak{z})$. — Le théorème suivant est très important, il nous permet d'écrire les nombres du corps sous une forme intéressante.

Théorème. — On peut toujours, et d'une infinité de manières, choisir trois nombres ω_1, ω_2, ω_3, tels que tout nombre entier du corps puisse être mis sous la forme

$$x\omega_1 + y\omega_2 + z\omega_3.$$

x, y, z étant des entiers rationnels.

Démonstration : La démonstration se décompose en deux parties. On établit d'abord la forme générale sous laquelle on peut écrire les entiers du corps, et on en déduit trois nombres répondant à la question.

Soit a, b, c trois entiers rationnels, il en résulte que les nombres algébriques $a + b\mathfrak{z} + c\mathfrak{z}^2$ sont entiers.

Soient maintenant a, b, c trois nombres rationnels quelconques, et soit

$$\alpha = a + b\mathfrak{z} + c\mathfrak{z}^2,$$

quelles conditions doivent remplir a, b, c pour que α soit un entier du corps. Si α est un entier les conjugués α' et α'' sont aussi entiers. Calculons a, b, c en fonction de α, α', α''

$$(1) \qquad \begin{cases} a + b\mathfrak{z} + c\mathfrak{z}^2 = \alpha \\ a + b\mathfrak{z}' + c\mathfrak{z}'^2 = \alpha' \\ a + b\mathfrak{z}'' + c\mathfrak{z}''^2 = \alpha'' \end{cases}$$

on a

$$(2) \qquad a = \frac{\begin{vmatrix} \alpha & \mathfrak{z} & \mathfrak{z}^2 \\ \alpha' & \mathfrak{z}' & \mathfrak{z}'^2 \\ \alpha'' & \mathfrak{z}'' & \mathfrak{z}''^2 \end{vmatrix}}{\begin{vmatrix} 1 & \mathfrak{z} & \mathfrak{z}^2 \\ 1 & \mathfrak{z}' & \mathfrak{z}'^2 \\ 1 & \mathfrak{z}'' & \mathfrak{z}''^2 \end{vmatrix}} = \frac{\begin{vmatrix} \alpha & \mathfrak{z} & \mathfrak{z}^2 \\ \alpha' & \mathfrak{z}' & \mathfrak{z}'^2 \\ \alpha'' & \mathfrak{z}'' & \mathfrak{z}''^2 \end{vmatrix} \begin{vmatrix} 1 & \mathfrak{z} & \mathfrak{z}^2 \\ 1 & \mathfrak{z}' & \mathfrak{z}'^2 \\ 1 & \mathfrak{z}'' & \mathfrak{z}''^2 \end{vmatrix}}{\begin{vmatrix} 1 & \mathfrak{z} & \mathfrak{z}^2 \\ 1 & \mathfrak{z}' & \mathfrak{z}'^2 \\ 1 & \mathfrak{z}'' & \mathfrak{z}''^2 \end{vmatrix}^2},$$

et des expressions analogues pour b et c.

Les nombres rationnels sont donc égaux à des fractions, dont les numérateurs et les dénominateurs sont des fonctions entières rationnelles symétriques de α, α', α'', z, z', z''. Les dénominateurs sont égaux à $d(z)$, ce sont des entiers rationnels, les numérateurs sont rationnels et par suite entiers.

Autrement si $\alpha = a + bz + cz^2$ est un entier, les dénominateurs de a, b, c rendus irréductibles ne peuvent avoir d'autres facteurs premiers que ceux de $d(z)$. On peut toujours prendre a, b, c sous la forme

$$a = \frac{A}{d(z)}, \qquad b = \frac{B}{d(z)}, \qquad c = \frac{C}{d(z)},$$

où A, B, C sont des entiers rationnels.

On a donc

$$(3) \qquad \alpha = \frac{A + Bz + Cz^2}{d(z)},$$

ce qui nous permettra de trouver ω_1, ω_2, ω_3.

Ecrivons tous les nombres entiers du corps sous la forme

$$\frac{a + bz + cz^2}{d(z)},$$

où a, b, c sont des entiers rationnels ; il y a certainement une infinité de nombres du corps pour lesquels le coefficient c de z^2 n'est pas nul. Tout nombre $\frac{a + bz + cz^2}{d(z)}$ peut être décomposé en deux parties. Divisons a, b, c par $d(z)$ et supposons les restes en valeur absolue $\leqq d(z)$, c'est-à-dire posons $a = a_1 d(z) + A$, on a

$$\frac{a + bz + cz^2}{d(z)} = a_1 + b_1 z + c_1 z^2 + \frac{A + Bz + Cz^2}{d(z)} = \alpha_1 + \alpha,$$

α_1 et α sont des entiers du corps. Nous ne considérons dans ce qui suit que les nombres entiers $\frac{A + Bz + Cz^2}{d(z)}$, pour lesquels les coefficients A, B, C sont en valeur absolue $\leqq |\, d(z) \,|$ (y compris le cas de l'égalité). Soit C^* le plus grand commun diviseur de tous les coefficients C, C est donc un nombre déterminé $\geqq 1$, il y a aussi dans les corps des nombres de la forme

$$\alpha^* = \frac{A^* + B^* z + C^* z^2}{d(z)},$$

car si

$$\alpha_1 = \frac{a_1 + b_1\vartheta + c_1\vartheta^2}{d(\vartheta)}, \qquad \alpha_2 = \frac{a_2 + b_2\vartheta + c_2\vartheta^2}{d(\vartheta)}$$

satisfaisant aux conditions indiquées et si t est le plus grand commun diviseur de c_1 et de c_2 il existe deux entiers u et v tels que $uc_1 + vc_2 = t$, et par suite

$$u\alpha_1 + v\alpha_2 = \frac{(ua_1 + va_2) + (ub_1 + vb_2)\vartheta + t\vartheta^2}{d(\vartheta)}.$$

Le nombre $u\alpha_1 + v\alpha_2$ est également un entier du corps. Si l'on combine de la même façon tous les nombres

$$\alpha = \frac{A + B\vartheta + C\vartheta^2}{d(\vartheta)},$$

dont le nombre est limité, on peut choisir les multiplicateurs u, v, w, ... de bien des façons différentes, de façon que le nombre entier α^* obtenu ait un coefficient déterminé C^* pour ϑ^2.

Le nombre C^* est un facteur de $d(\vartheta)$, car par hypothèse il y a parmi les nombres α le nombre ϑ^2 pour lequel $C = d(\vartheta)$. De plus si $\frac{a + b\vartheta + c\vartheta^2}{d(\vartheta)}$ désigne un entier quelconque du corps c est un multiple de C^* car $c = c_1 d(\vartheta) + C$.

Nous prendrons pour α^* un nombre déterminé, en supposant qu'on ait fixé non seulement la valeur de C^* mais qu'on ait choisi aussi A^* et B^*, et nous remplacerons α^* par ω_3. Alors tout nombre

$$\alpha = \frac{a + b\vartheta + c\vartheta^2}{d(\vartheta)}$$

peut s'écrire

$$\alpha = \frac{a_1 + b_1\vartheta}{d(\vartheta)} + z\omega_3,$$

où z est un entier rationnel et $\frac{a_1 + b_1\vartheta}{d(\vartheta)}$ un entier du corps.

Nous supposerons encore que dans

$$\beta = \frac{A_1 + B_1\vartheta}{d(\vartheta)} \tag{5}$$

ne représente que les entiers dont les coefficients sont en valeur absolue $\leqq |d(\mathfrak{I})|$. Opérons comme précédemment et soit B_1^* le plus grand commun diviseur de tous les B_1 qui sont en nombre fini, il en résulte que le corps contient toujours un entier de la forme

$$(6) \qquad \beta^* = \frac{A_1^* + B_1^*\mathfrak{I}}{d(\mathfrak{I})}.$$

B_1^* est un facteur de $d(\mathfrak{I})$ et si $\frac{a_1 + b_1\mathfrak{I}}{d(\mathfrak{I})}$ représente un entier du corps b_1 est un multiple de B_1^*.

Supposons que dans (6) A^* soit également un nombre déterminé et posons $\beta^* = \omega_2$, tout nombre

$$\beta = \frac{a_1 + b_1\mathfrak{I}}{d(\mathfrak{I})}$$

peut se mettre sous la forme

$$\beta = A_2 + y\omega_2,$$

où A_2 et y sont des entiers rationnels.

Si enfin l'on pose $\omega_1 = 1$, les trois nombres ω_1, ω_2, ω_3 répondent aux conditions de l'énoncé. Tout entier α du corps peut être mis sous la forme

$$(7) \qquad \alpha = x\omega_1 + y\omega_2 + z\omega_3.$$

Car on peut d'abord choisir z entier et rationnel, de façon que $\alpha - z\omega_3$ ait la forme β de l'équation (5). Ensuite on peut choisir y entier et rationnel tel que

$$\beta - y\omega_2 = \gamma$$

soit un nombre rationnel. On peut donc poser $\gamma = x\omega_1 = x$. On dit que trois nombres ayant les mêmes propriétés que

$$\omega_1, \quad \omega_2, \quad \omega_3$$

forment *une base du corps*.

Au lieu des nombres ω_1, ω_2, ω_3 on peut choisir

$$\omega = 1, \quad \omega_1 = \frac{B + B_1\mathfrak{I}}{d(\mathfrak{I})}, \quad \omega_2 = \frac{C + C_1\mathfrak{I} + C_2\mathfrak{I}^2}{d(\mathfrak{I})}$$

comme *base normale*, tels que $|B|, |C|, |C_1| < |d(\vartheta)|$, c'est-à-dire correspondent aux plus petites valeurs de A_1^* dans l'égalité (6). Nous avons écrit pour simplifier $B_1 = B_1^*$, $C_2 = C^*$.

Si $\omega_1, \omega_2, \omega_3, \omega_1^*, \omega_2^*, \omega_3^*$ désignent deux bases différentes, ces nombres sont liés par des relations linéaires à coefficients entiers rationnels

$$(8) \qquad \begin{cases} \omega_1^* = a_{11}\omega_1 + a_{12}\omega_2 + a_{13}\omega_3, \\ \omega_2^* = a_{21}\omega_1 + a_{22}\omega_2 + a_{23}\omega_3, \\ \omega_3^* = a_{31}\omega_1 + a_{32}\omega_2 + a_{33}\omega_3. \end{cases}$$

Comme réciproquement les ω peuvent s'exprimer de la même manière en fonction des ω^*, cela exige que

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = \pm 1.$$

D'autre part si l'on choisit les a_{ik} entiers rationnels satisfaisant à cette condition, les 3 équations (8) nous fourniront une nouvelle base. Or le choix des a_{ik} est possible d'une infinité de manières, il existe donc une infinité de systèmes de trois nombres formant une base du corps.

Le déterminant

$$(9) \qquad d = \begin{vmatrix} \omega_1 & \omega_2 & \omega_3 \\ \omega_1' & \omega_2' & \omega_3' \\ \omega_1'' & \omega_2'' & \omega_3'' \end{vmatrix}^2$$

est le *Discriminant du corps*.

Le théorème relatif à la multiplication des déterminants nous montre que

$$(\omega_1^*, \omega_2^*, \omega_3^*)^2 = (a_{11}, a_{22}, a_{33})^2 (\omega_1, \omega_2', \omega_3'')^2 = d \text{ [1]}.$$

Le discriminant du corps est indépendant de la base.

Le discriminant du corps est un nombre rationnel.

---

[1] Nous avons représenté un déterminant par les éléments de la diagonale qui va de gauche à droite.

Ce nombre est un diviseur commun des discriminants de tous les entiers du corps, car on a

$$d(\alpha) = (x, y_1, z_2)^2 . d,$$

en supposant

$$(10) \quad \begin{cases} 1 = x\omega_1 + y\omega_2 + z\omega_3, \\ \alpha = x_1\omega_1 + y_1\omega_2 + z_1\omega_3, \\ \alpha^2 = x_2\omega_1 + y_2\omega_2 + z_2\omega_3. \end{cases}$$

Désignons par ω, ω_1, ω_2 une base normale

$$\omega = 1, \qquad \omega_1 = \frac{B + B_1\vartheta}{d(\vartheta)}, \qquad \omega_2 = \frac{C + C_1\vartheta + C_2\vartheta^2}{d(\vartheta)}.$$

On a

$$(11) \qquad d = \frac{B_1^2 C_2^2}{d(\vartheta)^3}.$$

On a déjà montré que B_1 et C_2 sont des diviseurs de $d(\vartheta)$ et ceci nous montre encore que d n'admet que des facteurs contenus dans $d(\vartheta)$.

De plus ce quotient nous montre que d contient certainement en facteurs, les nombres premiers figurant dans $d(\vartheta)$ à une puissance impaire.

Lorsque le discriminant d du corps est égal à $d(\vartheta)$, on voit en remplaçant α par ϑ dans le système (10) que $(x, y_1, z_2) = \pm 1$, c'est-à-dire que les trois nombres 1, ϑ, ϑ^2 forment une base du corps.

Une discussion plus approfondie du fait que $\frac{d(\vartheta)}{d}$ sont des entiers rationnels nous montrerait que $d = d(\vartheta)$ toutes les fois que $d(\vartheta)$ ne contient ses facteurs premiers qu'à la première puissance.

$d(\vartheta)$ ne peut être égal à ± 1, d'après la valeur de d on voit qu'il ne peut être égal à ± 1 tant que $d(\vartheta)$ n'est pas carré parfait. Il pourrait encore être égal à ± 1 lorsque $d(\vartheta) = \pm r^2$. Mais le théorème de Minkowski permet de démontrer que le discriminant de tout corps est différent de ± 1. On démontre d'abord que dans tout corps il existe un nombre α, tel que $|n(\alpha)| < \sqrt{|d|}$ et comme $n(\alpha) \geqq 1$ il faut que $|d| > 1$. Ceci est développé au chap. VI, § 18 du Bericht. de M. Hilbert.

42. Le calcul des bases du corps $k(\mathfrak{z})$. — Le calcul d'une base d'un corps cubique n'est plus aussi simple que celui d'une base du corps quadratique. Cependant (en s'appuyant sur les théorèmes relatifs aux discriminants des nombres entiers) mettre la base du corps sous une forme, telle que le calcul numérique de ces bases dans les cas particuliers devienne assez facile (¹).

Soit d'abord la base

$$\omega = 1, \qquad \omega_1 = \frac{B + B_1\mathfrak{z}}{d(\mathfrak{z})}, \qquad \omega_2 = \frac{C + C_1\mathfrak{z} + C_2\mathfrak{z}^2}{d(\mathfrak{z})}.$$

De plus posons

$$d(\mathfrak{z}) = \pm q_1^{6e_1} \dots q^{6e} p_1^{f_1} \dots p^{f} \quad (d(\mathfrak{z}) \neq \pm 1),$$

où $e_1 \dots e$ sont des entiers quelconques $\geqq 0$, $f_1 \dots f$ ne peuvent représenter que les nombres 1, 2, ... 5.

Mais le discriminant de ω_1 est

$$d(\omega_1) = \frac{B_1^6}{d(\mathfrak{z})^3},$$

$d(\omega_1)$ est un nombre entier $\neq \pm 1$, B_1 ne contient que des facteurs premiers de $d(\mathfrak{z})$, on peut donc poser

$$B_1 = b^* q_1^{3e_1} \dots q^{3e} p_1^{f_1} \dots p^{f} = b^* b_1^*.$$

où b^* égale ± 1 ou égale un nombre divisible par les facteurs premiers q, p.

Mais alors

$$\omega_1 = \frac{B + b^* q_1^{3e_1} \dots q^{3e} p_1^{f_1} \dots p^{f}\mathfrak{z}}{d(\mathfrak{z})}.$$

mais

$$b = q_1^{e_1} \dots q^{e}\omega_1 \mp b^*\mathfrak{z} = \frac{B \cdot q_1^{e_1} \dots q^{e}}{d(\mathfrak{z})} = \frac{B}{\pm b_1^*}$$

est un nombre entier rationnel, il faut que B soit divisible par b_1^*, par suite ω_1 est de la forme

$$\omega_1 = \frac{b + b^*\mathfrak{z}}{q_1^{e_1} \dots q^{e}}.$$

(¹) Les résultats de ce paragraphe sont cités dans la dissertation de W. L. Reid, *Tafeln der Klassenanzahlen für kübische Zahlkörper*, Gött., 1899, comme dus à Woronoj (*Fortsch. der Math.*, Bd. XXV, Jahrgurz, 1894).

Si l'on considère que $x\omega_1 + y\mathfrak{z}$ est un nombre entier lorsque x et y sont des entiers rationnels, on en déduit facilement que b^* est un diviseur de $q_1^{e_1}\dots q^{e}$, c'est-à-dire qu'il ne contient pas d'autres facteurs premiers que $q_1 \dots q$; car on peut déterminer x et y tels que $xb^* + yq_1^{e_1}\dots q^{e}$ soit le plus grand commun diviseur de b^* et de $q_1^{e_1}\dots q^{e}$.

De l'égalité $q_1^{e_1}\dots q^{e}\omega_1 - b^*\mathfrak{z} = b^*\alpha = b$ il résulte que b est divisible par b^*. En simplifiant par b^* les deux termes du numérateur on a

$$\omega_1 = \frac{b_1 + \mathfrak{z}}{D},$$

ou encore en récrivant b au lieu de b_1

(1) $$\omega_1 = \frac{b + \mathfrak{z}}{D},$$

où $D = q_1^{r_1}\dots q^{r}$ est un entier rationnel qui est contenu ainsi que tous ses facteurs premiers au moins à la sixième puissance dans $d(\mathfrak{z})$. Si $d(\mathfrak{z})$ ne contient aucun facteur à la sixième puissance ou à une puissance supérieure $D = 1$, et l'on peut poser $\omega_1 = \mathfrak{z}$.

Pour faciliter ce qui suit nous écrirons

$$d(\mathfrak{z}) = \pm D^2 D,$$

et

$$\omega_2 = \frac{C + C_1\mathfrak{z} + C_2\mathfrak{z}^2}{D^2\overline{D}}.$$

On obtiendra des valeurs plus précises de C, C_1, C_2 en combinant

$$\omega_1^2 = \frac{b^2 + 2b\mathfrak{z} + \mathfrak{z}^2}{D^2}$$

avec ω_2. Déterminons x et y de façon que dans l'entier

$$x\omega_1^2 + y\omega_2$$

le coefficient de $\mathfrak{z}^2$ soit un diviseur D_2 de $\overline{D}$. Soit $\overline{D} = D_1D_2$ alors

$$\omega_2 = \frac{C + C_1\mathfrak{z} + D_2\mathfrak{z}^2}{D^2D_1D_2}.$$

Il existe trois nombres entiers rationnels u, v, w qui satisfont à

$$(2)\qquad \omega_1^2 = u + v\omega_1 + w\omega_2,$$

d'où

$$(2_a)\qquad w = D_1,\quad C_1 = D_2(2b - vD),\quad C = D_2(b^2 - uD^2 - vbD),$$

c'est-à-dire que C et C_1 sont divisibles par D_2,

$$C_1 = D_2 c_1,\qquad C = D_2 c,$$

d'où

$$(3)\qquad \omega_2 = \frac{c + c_1\vartheta + \vartheta^2}{D^2 D_1}.$$

Pour restreindre le choix de b, c, c_1 nous remarquerons que ω_1, ω_2 sont des nombres entiers, par suite b doit satisfaire aux congruences

$$(4)\qquad 3b - a_1 \equiv 0\ (D),$$

$$(5)\qquad 3b^2 - 2a_1 b + a_2 \equiv 0\ (D^2),$$

$$(6)\qquad b^3 - a_1 b^2 + a_2 b + a_3 \equiv 0\ (D^3).$$

(a_1, a_2, a_3 sont les coefficients entiers de l'équation qui définit ϑ).

La première de ces trois congruences nous permet de prendre pour ω_1 l'un des trois nombres

$$\frac{b - \vartheta}{D},\quad \frac{a_1 - 2b + \vartheta}{D},\quad \frac{a_1 - 2b - vD + \vartheta}{D} = \frac{a_1 - c_1 + \vartheta}{D},$$

en tenant compte de (2_a).

Soit

$$(7)\qquad \omega_1 = \frac{a_1 - c_1 + \vartheta}{D}.$$

Dans (2) au lieu de prendre ω_1^2 prenons

$$\omega_1^2 - \frac{3b - a_1}{D}\, v - k,$$

et tenant encore compte de (4) on peut déterminer k de telle sorte que

$$c = c_1^2 - a_1 c_1 + a_2.$$

Si enfin on remplace c_1 par A on voit qu'on peut écrire

$$(8)\quad \omega = 1, \quad \omega_1 = \frac{-A + a_1 + z}{D}, \quad \omega_2 = \frac{A^2 - a_1 A + a_2 + Az - z^2}{D^2 D_1}$$

où il nous reste à déterminer AD et D_1.

En adoptant cette base on a

$$d = \frac{1}{D^4 D_1^2} d(z),$$

c'est-à-dire que le carré de D_1 doit être contenu dans $d(z)$.

En écrivant que ω_1 est un entier ou que

$$\omega_1 + \omega_1' + \omega_1'', \quad \omega_1\omega_1' + \omega_1'\omega_1'' + \omega_1''\omega_1 \quad \text{et} \quad \omega_1\omega_1'\omega_1''$$

sont des entiers rationnels on obtient trois congruences. Elles résultent de (4), (5) et (6) lorsqu'on y remplace b par $-A + a_1$. Ces congruences sont en partie comprises dans celles qu'on obtient en exprimant que ω_2 est entier.

Pour que $\omega_2 + \omega_2' + \omega_2''$ soit entier il faut que

$$3(A - a_1)^2 + 2a_1(A - a_1) + a_2 \equiv 0, \quad (D^2 D_1).$$

Un calcul simple nous montre que

$$\omega_1\omega_2 = -\frac{G(A - a_1)}{D^3 D_1},$$

où

$$G(x) = x^3 + a_1 x^2 + a_2 x + a_3,$$

et par suite

$$\omega_1\omega_1'\omega_1'' \cdot \omega_2\omega_2'\omega_2'' = -\frac{[G(A - a_1)]^3}{D^9 D_1^3},$$

comme d'autre part la congruence (3) exige que

$$\omega_1\omega_1'\omega_1'' = -\frac{G(A - a_1)}{D^3},$$

il reste

$$[G(A - a_1)]^2 \equiv 0, \quad (D^6 D_1^2).$$

elle n'est satisfaite que si

$$G(A - a_1) = (A - a_1)^3 + a_1(A - a_1)^2 + a_2(A - a_1) + a_3 \equiv 0, \quad (D^3 D_1^2),$$

Enfin si on écrit que $\omega_2\omega_2' + \omega_2'\omega_2'' + \omega_2''\omega_2$ est un entier, on trouve que

$$\{3(A - a_1) + a_1\}\{6(A - a_1)\} \equiv 0, \qquad (D^4D_1),$$

elle n'est pas nouvelle, elle est le produit de (4) et de la dernière congruence que nous venons d'obtenir.

Le résultat de ces considérations peut être résumé ainsi :

La base du corps $k(\mathfrak{z})$ déterminée par une racine $\mathfrak{z}$ de l'équation

$$G(x) = x^3 + a_1x^2 + a_2x + a_3 = 0$$

est

$$\omega = 1, \quad \omega_1 = \frac{-(A - a_1) + \mathfrak{z}}{D}, \quad \omega_2 = \frac{(A - a_1)^2 + a_1(A - a_1) + a_2 + A\mathfrak{z} + \mathfrak{z}^2}{D^2D_1},$$

où D^6 et D_1^2 au moins sont contenus dans $d(\mathfrak{z})$ et où A, D, D_1 sont des entiers rationnels satisfaisant aux congruences

$$3(A - a_1) + a_1 \equiv 0, \qquad (D)$$

$$3(A - a_1)^2 + 2a_1(A - a_1) + a_2 \equiv 0, \qquad (D^2D_1)$$

$$(A - a_1)^3 + a_1(A - a_1)^2 + a_2(A - a_1) + a_3 \equiv 0, \qquad (D^3D_1^2).$$

On pourrait encore indiquer d'autres conditions pour D, nous les passerons sous silence, le lecteur les trouvera.

Appliquons ce qui précède à l'exemple le plus simple, soit $\mathfrak{z}$ une racine de

$$G(x) = x^3 + a_3 = 0.$$

Supposons que a_3 ne contienne aucun nombre premier au cube, et soit N le produit de tous les nombres premiers qui entrent au carré dans a_3. Alors on a pour la base du corps les cas possibles suivants :

1. $a_3 \equiv 0\ (3)$

$$\omega = 1, \qquad \omega_1 = \mathfrak{z}, \qquad \omega_2 = \frac{\mathfrak{z}^2}{N}.$$

2. $a_3 \not\equiv 0\ (3)$, mais $a_3 \equiv \pm 2$ ou $a_3 \equiv \pm 4\ (9)$,

$$\omega = 1, \qquad \omega_1 = \mathfrak{z}, \qquad \omega_2 = \frac{\mathfrak{z}^2}{N}.$$

3. $a_3 \equiv 1\ (9)$.

$$\omega = 1, \quad \omega_1 = z, \quad \omega_2 = \frac{N + Nz + z^2}{3N} \quad \text{pour} \quad N \equiv 1\ (3),$$

$$\omega = 1, \quad \omega_1 = z, \quad \omega_2 = \frac{-N - Nz + z^2}{3N} \quad \text{pour} \quad N \equiv -1\ (3).$$

4. $a_3 \equiv -1\ (9)$.

$$\omega = 1, \quad \omega_1 = z, \quad \omega_2 = \frac{N - Nz + z^2}{3N} \quad \text{pour} \quad N \equiv -1\ (3),$$

$$\omega = 1, \quad \omega_1 = z, \quad \omega_2 = \frac{-N - Nz + z^2}{3N} \quad \text{pour} \quad N \equiv -1\ (3).$$

Nous ferons $N = 1$ si a_3 ne contient aucun facteur au carré.

Le cas où a_3 contiendrait des facteurs à la troisième puissance (d'une façon générale à la puissance $3\nu \pm 1$) se ramène au cas particulier précédent. Si $a_3' = p^3 . a_3$ on pose $x = py$ et on étudie $y^3 - a_3 = 0$ au lieu de $x^3 - a_3' = 0$.

43. Les idéaux du corps $k(z)$ et leur décomposition. — Nous dirons encore qu'un nombre entier α est divisible par un entier β, s'il existe un entier γ tel que

$$\alpha = \beta . \gamma.$$

Nous ne tiendrons pas compte des facteurs qui divisent 1 et que nous nommerons des unités. Si l'on tient compte du théorème relatif aux normes un nombre α ne peut contenir qu'un nombre limité de facteurs. La décomposition d'un nombre en facteurs indécomposables est encore possible de plusieurs manières.

Pour simplifier cette décomposition nous aurons encore recours aux idéaux. Comme le corps quadratique le corps cubique sera l'ensemble de ses nombres et de ses idéaux.

Il suffit d'étendre les considérations du chapitre II, n° 9.

Définition : Un idéal $\mathfrak{j}$ est l'ensemble (le système) illimité des entiers du corps $k(z)$

$$\mathfrak{j} = (\alpha, \beta, \gamma, \ldots).$$

tel que toute combinaison linéaire $\lambda_1\alpha + \lambda_2\beta + \lambda_3\gamma + \ldots$ des nombres $\alpha, \beta, \gamma, \ldots$ avec des nombres quelconques entiers du corps appartienne à $\mathfrak{j}$.

D'où les remarques :

1. Tout idéal contient le nombre 0.

2. Un idéal contient toujours outre le nombre α le nombre entier rationnel $n(\alpha)$, car $\alpha'\alpha''$ est un entier du corps $k(\vartheta)$. Tout idéal contient donc une infinité de nombres entiers rationnels.

3. Lorsqu'un idéal contient α qui divise 1, il contient 1 et l'idéal est un *idéal unité*.

4. Lorsque tous les nombres d'un idéal sont divisibles par un nombre appartenant à l'idéal, par exemple α, on a un *idéal principal* et on l'écrit

$$\mathfrak{j} = (\alpha).$$

On peut répéter le raisonnement qui a démontré l'existence d'une base de corps et on obtient le

Théorème. — Dans tout idéal $\mathfrak{j}$ du corps $k(\vartheta)$ on peut choisir d'une infinité de manières trois nombres i_1, i_2, i_3 tels que tout autre nombre de l'idéal puisse être mis sous la forme

$$xi_1 + yi_2 + zi_3,$$

où x, y, z sont des entiers rationnels.

Les trois nombres i_1, i_2, i_3 forment une *base de l'idéal*.

On peut encore choisir une base normale telle que

$$\iota_1 = \iota, \qquad \iota_2 = \iota_1 + \iota_1^{(1)}\omega_1, \qquad \iota_3 = \iota_2 + \iota_2'^{(1)}\omega_1 + \iota_2'^{(2)}\omega_2,$$

on écrit

$$\mathfrak{j} = (\iota_1, \iota_2, \iota_3)$$

ou

$$\mathfrak{a} = (\alpha_1, \alpha_2, \alpha_3), \text{ etc.}$$

Si les nombres a_{rs} satisfont à $(a_{11}, a_{22}, a_{33}) = \pm 1$ et il y a une infinité de nombres répondant à la question, les trois nombres

$$i_r^* = a_{r1}i_1 + a_{r2}i_2 + a_{r3}i_3 \quad (r = 1, 2, 3).$$

forment encore une base de l'idéal $\mathfrak{j}$, il y a donc une infinité de systèmes de trois nombres d'un idéal, formant une base de cet idéal.

Toutes les fois qu'il s'agit de lois de divisibilité dans le corps,

les idéaux remplacent les nombres entiers. On peut étendre aux idéaux la multiplication et la division des entiers, mais non pas l'addition. On a les définitions suivantes :

Définition : Soient $\mathfrak{a}$ et $\mathfrak{b}$ deux idéaux du corps

$$\mathfrak{a} = (\alpha_1, \alpha_2, \alpha_3, \ldots), \qquad \mathfrak{b} = (\beta_1, \beta_2, \beta_3, \ldots).$$

On entend par produit de ces deux idéaux l'idéal $\mathfrak{c}$ contenant le système des nombres obtenus en multipliant chaque nombre de $\mathfrak{a}$ par chaque nombre de $\mathfrak{b}$ et en y ajoutant toutes les combinaisons linéaires de ces produits et d'entiers quelconques λ_1, λ_2, ... du corps $k(\mathfrak{z})$.

On écrit $\mathfrak{c} = \mathfrak{a} \cdot \mathfrak{b}$.

Réciproquement $\mathfrak{c}$ est dit divisible par $\mathfrak{a}$, s'il existe un idéal $\mathfrak{b}$, tel que $\mathfrak{c} = \mathfrak{a} \cdot \mathfrak{b}$.

Une conséquence immédiate de cette définition est évidemment la suivante : Lorsqu'un idéal $\mathfrak{c}$ est divisible par un idéal $\mathfrak{a}$, tout nombre de $\mathfrak{c}$ est contenu dans $\mathfrak{a}$.

Un idéal différent de (1) qui n'est divisible que par lui-même et par des idéaux unités, est un idéal premier.

Définition : Deux idéaux $\mathfrak{a}$ et $\mathfrak{b}$ sont dits équivalents s'il existe dans $k(\mathfrak{z})$ deux nombres tels que

$$\mathfrak{a}(\alpha) = \mathfrak{b}(\beta),$$

ce qu'on écrit

$$\frac{\mathfrak{a}}{\mathfrak{b}} = \frac{\alpha}{\beta}.$$

Le lecteur formulera lui-même ici les théorèmes relatifs à l'équivalence que nous avons traités au n° 16.

La notion d'équivalence permet encore de répartir les idéaux en classes. Tous les idéaux équivalents forment une classe.

Nous arrivons maintenant au théorème fondamental de la décomposition unique des idéaux. Nous suivrons ici la deuxième méthode due à M. Hurwitz [1].

---

[1] A. Hurwitz. — *Nachr. von der kgl. Ges. d. Wissensch. zu Gött.*, 1895. S. 323. Dans cette façon d'établir la théorie des idéaux le théorème de la décomposition unique est une conséquence de ce que le nombre des classes est limité. C'est là un fait merveilleux. P. Furtwangler est arrivé à un résultat analogue mais par d'autres moyens. *Ibid.*, S. 381.

Lemme. — Un nombre α du corps dont la norme $\pm a$ est finie ne peut être contenu que dans un nombre fini d'idéaux distincts.

Démonstration : Soit

$$\mathfrak{a} = (\alpha_1, \alpha_2, \alpha_3, \dots \alpha \dots),$$

et soit a un nombre rationnel de l'idéal. Soit $\omega_1 = 1$, ω_2, ω_3 une base du corps et soit

$$\iota_1 = i, \qquad \iota_2 = i_1 + i_1'^{(1)}\omega_2, \qquad \iota_3 = i_1 + i_2'^{(1)}\omega_1 + i_2''^{(2)}\omega_2$$

une base normale de l'idéal i, i_1, ... $i_2''^{(2)}$ sont des entiers du système complet des restes suivant le module a. En effet a appartenant à l'idéal $a\omega_1$, $a\omega_2$, $a\omega_3$ appartiennent à l'idéal $\mathfrak{a}$ et par suite i, $i_1^{(1)}$, $i_2^{(2)}$ sont des diviseurs de a. Comme d'autre part $|i|$ n'est pas plus petit que les valeurs absolues des autres coefficients depuis i_1 jusqu'à i_2^2 notre affirmation est exacte. En remplaçant i jusqu'à i_2^2 par toutes les combinaisons possibles des plus petits restes suivant a on obtient un nombre fini de bases différentes et par suite d'idéaux différents.

Théorème. — Un idéal ne peut avoir qu'un nombre fini de diviseurs idéaux.

Il suffit de considérer le lemme précédent et de remarquer que tout nombre compris dans le dividende doit aussi être contenu dans le diviseur.

Lemme. — Le nombre des classes d'idéaux distincts du corps $k(\vartheta)$ est fini (tout idéal du corps est équivalent à un idéal au moins, qui contient un nombre fini entier et rationnel, dont la valeur ne dépend que du discriminant du corps).

Démonstration : Il est nécessaire de distinguer les corps réels et les corps imaginaires.

Soit d'abord $k(\vartheta)$ un corps réel et

$$\mathfrak{a} = (\alpha_1, \alpha_2, \alpha_3)$$

un idéal quelconque dont la base est

$$\alpha_i = a_{i1}\omega_1 + a_{i2}\omega_2 + a_{i3}\omega_3 \qquad (\text{pour } i = 1, 2, 3).$$

Supposons qu'on ait formé les normes de tous les nombres de $\mathfrak{a}$, ces normes prises en valeur absolue forment une suite de nombres parmi lesquels un est plus petit que tous les autres. Soit ι le nombre

de l'idéal qui a cette plus petite norme. Ceci posé nous affirmons qu'il existe un nombre A fini, entier, rationnel, qui ne dépend que de la valeur du discriminant du corps, et tel que $A\alpha$ soit divisible par ι, α étant un nombre quelconque du corps.

En effet soit α_i un des trois nombres de base, le théorème de Minkowski nous permet de déterminer quatre entiers rationnels x, y, z, u qui ne sont pas tous nuls, satisfaisant à

$$\begin{aligned} &|\alpha_i u + \iota\omega_1 x + \iota\omega_2 y + \iota\omega_3 z| \leqq \varkappa_2 \\ &|\alpha_i' u + \iota'\omega_1' x + \iota'\omega_2' y + \iota'\omega_3' z| \leqq \varkappa_3 \\ &|\alpha_i'' u + \iota''\omega_1'' x + \iota''\omega_2'' y + \iota''\omega_3'' z| \leqq \varkappa_1 \\ &\left|\frac{\pm \alpha_i u}{\sqrt{d}}\right| \leqq \varkappa_4. \end{aligned}$$

où $\varkappa_1$, $\varkappa_2$, $\varkappa_3$, $\varkappa_4$ sont quatre nombres positifs dont le produit est égal au déterminant des quatre formes pris positivement

$$\varkappa_1\varkappa_2\varkappa_3\varkappa_4 = \frac{\pm \alpha_i}{\sqrt{d}}\, n(\iota) \begin{vmatrix} \omega_1 & \omega_2 & \omega_3 \\ \omega_1' & \omega_2' & \omega_3' \\ \omega_1'' & \omega_2'' & \omega_3'' \end{vmatrix} = \pm \alpha_i n(\iota).$$

Si l'on prend comme c'est permis $\varkappa_4 = 2\,|\alpha_i|$ et par suite $|u| \leqq |2\sqrt{d}|$, et si l'on pose

$$\beta = \alpha_i u + \iota(\omega_1 x + \omega_2 y + \omega_3 z),$$

β est un entier dont la norme

$$n(\beta) \leqq \varkappa_1\varkappa_2\varkappa_3,$$

et comme $\varkappa_1\varkappa_2\varkappa_3 = \frac{1}{2}\, n(\iota)$

$$n(\beta) \leqq \frac{1}{2}\, n(\iota),$$

β est un nombre de l'idéal $\mathfrak{a}$, car c'est une combinaison de nombres de l'idéal α_i et ι avec des entiers du corps, car u et $\omega_1 x + \omega_2 y + \omega_3 z = \lambda$ sont des entiers. De plus u ne peut être nul car λ n'est pas nul et on aurait

$$n(\beta) = |\, n(\iota)\, n(\omega_1 x + \omega_2 y + \omega_3 z)\,| \leqq \frac{1}{2}\, |\, n(\iota)\,|,$$

c'est-à-dire

$$n(\lambda) \leqq \frac{1}{2},$$

c'est-à-dire que $n(\omega_1 x + \omega_2 y + \omega_3 z)$ ne pourrait être entier, ce qui est impossible car $n(\lambda)$ est un entier $\geqslant 1$.

Mais ι est le nombre de l'idéal de plus petite norme, il faut donc que $n(\beta) = 0$ et par suite $\beta = 0$, c'est-à-dire

$$\alpha_i u + \lambda \iota = 0,$$

ce qu'on peut exprimer ainsi. Etant donné un nombre α_i on peut trouver un entier rationnel $|u| < |2\sqrt{d}|$ tel que $\alpha_i u$ soit divisible par ι.

Ce facteur u n'est pas nécessairement le même pour les trois nombres α_i et il n'est certainement pas le même pour les idéaux différents $\mathfrak{a}$, $\mathfrak{a}_1$, etc. Désignons par A le produit de tous les nombres positifs entiers rationnels $< 2|\sqrt{d}|$ les produits des trois nombres de bases $A\alpha_1$, $A\alpha_2$, $A\alpha_3$ sont divisibles par ι, et par suite pour tout entier α de l'idéal le produit $A\alpha$ est divisible par ι.

En tenant compte de la loi qui précède

$$(A)\alpha = (A\alpha_1, A\alpha_2, A\alpha_3, A\iota, \ldots) = \iota(\lambda_1, \lambda_2, \lambda_3, A, \ldots),$$

c'est-à-dire

$$(A)\mathfrak{a} = (\iota)\mathfrak{b}$$

ou encore

$$\mathfrak{a} = \mathfrak{b},$$

c'est-à-dire que tout idéal $\mathfrak{a}$ du corps est équivalent à un autre idéal $\mathfrak{b}$ qui contient A. A est un nombre fini lorsque d est fini. Mais il n'y a qu'un nombre fini d'idéaux qui contiennent A. Par suite il faut qu'il soit possible de trouver un nombre limité h d'idéaux

$$\mathfrak{b}_1\ \mathfrak{b}_2, \ldots, \mathfrak{b}_h,$$

tels que tout idéal $\mathfrak{a}$ du corps soit équivalent à l'un d'entre eux et à un seul. Ou encore :

Le nombre des classes du corps $k(\vartheta)$ est limité.

En second lieu soient $k(\vartheta)$ un corps imaginaire et supposons que $\mathfrak{a}$, α_i, α, ι aient le même sens que dans le cas du corps réel, seulement ici α_i, α sont des nombres imaginaires.

Nous chercherons encore à former un entier

$$\beta = \alpha_i u + i(\omega_1 x + \omega_2 y + \omega_3 z),$$

tel que

$$n(\beta) \leqq |n(\alpha_i)| \qquad \text{ou} \qquad \beta = 0.$$

Soit α_1 la racine conjuguée imaginaire de α, et α' sa racine conjuguée réelle, nous appliquerons le théorème de Minkowski aux quatre formes linéaires

$$\frac{1}{\sqrt{2}}(\beta + \beta'), \qquad \frac{1}{\sqrt{-2}}(\beta - \beta'), \qquad \beta'', \qquad \pm \frac{|\alpha_i| u}{\sqrt{d}},$$

de telle sorte que

$$\left| \frac{1}{\sqrt{2}}(\beta + \beta') \right| \leqq \varkappa_1$$

$$\left| \frac{1}{\sqrt{-1}\sqrt{2}}(\beta - \beta') \right| \leqq \varkappa_1$$

$$|\beta''| \leqq \varkappa_3$$

$$\left| \frac{\alpha_i u}{\sqrt{d}} \right| \leqq \varkappa_4$$

où nous poserons

$$\beta = \alpha_i u + \omega_1 x + \omega_2 y + \omega_3 z$$

et

$$\varkappa_1^2 \varkappa_3 \varkappa_4 = 2\,|\alpha_i n(\alpha)|.$$

Si l'on fait

$$\varkappa_4 = 4\,|\alpha_i|, \qquad \varkappa_1^2 \varkappa_3 = \frac{1}{2}\,|n(\alpha)|$$

$$|n(\beta)| = \left| \left\{ \frac{1}{2}(\beta + \beta') \right\}^2 + \left(\frac{1}{2\sqrt{-1}}(\beta - \beta') \right)^2 \beta'' \right|$$

$$= \left\{ \left(\frac{\varkappa_1}{\sqrt{2}} \right)^2 + \left(\frac{\varkappa_1}{\sqrt{2}} \right)^2 \right\} k_3$$

$$= \varkappa_1^2 \varkappa_3 < \frac{1}{2}\,|n(\alpha)|.$$

D'où nous tirerons les même conclusions que tout à l'heure. Donc d'une façon générale :

Le nombre h des classes de tout corps $k(\alpha)$ est un nombre fini.

Théorème. — Si $\mathfrak{a}$ est un idéal non principal du corps il existe toujours un idéal $\mathfrak{b}$ qui n'est pas non plus un idéal principal tel que le produit $\mathfrak{a} . \mathfrak{b}$ soit un idéal principal.

Démonstration : Soit $\mathfrak{a}$ un idéal non principal, formons

$$\mathfrak{a},\ \mathfrak{a}^2,\ \mathfrak{a}^3,\ \ldots$$

Ces puissances se répartissent en un nombre fini de classes, on peut admettre que $\mathfrak{a}^{m+h_1}$ est la première puissance qui est équivalente à une puissance inférieure $\mathfrak{a}^m$.

Soit donc

$$\mathfrak{a}^{m+h_1} \sim \mathfrak{a}^m$$

ou

$$(\alpha)\,\mathfrak{a}^{m+h_1} = (\beta)\,\mathfrak{a}^m$$

ou bien encore

$$(1) \qquad \mathfrak{a}^{m+h_1} = (\lambda)\,\mathfrak{a}^m,$$

où α, β sont des entiers du corps $k(\theta)$.

Il s'agit de montrer que $\mathfrak{a}^{h_1}$ est un idéal principal égal à (λ). Pour cela nous démontrerons que le nombre λ défini par l'égalité (1) est un nombre entier.

Pour cela nous remarquerons tout d'abord que tous les nombres de l'idéal $\mathfrak{a}^{m+h_1}$ sont des nombres de $\mathfrak{a}^m$, car on obtient $\mathfrak{a}^{m+h_1}$ en multipliant $\mathfrak{a}^m$ par $\mathfrak{a}^{h_1}$. Si alors on désigne par α_1, α_2, α_3 une base de l'idéal $\mathfrak{a}^m$, $\lambda\alpha_1$ est un nombre entier car c'est un nombre de l'idéal $\mathfrak{a}^{m+h_1}$, et alors $\lambda\alpha_1$ peut s'exprimer ainsi

$$\begin{aligned}
\lambda\alpha_1 &= x_1\alpha_1 + y_1\alpha_2 + z_1\alpha_3 \\
\lambda\alpha_2 &= x_2\alpha_1 + y_2\alpha_2 + z_2\alpha_3 \\
\lambda\alpha_3 &= x_3\alpha_1 + y_3\alpha_2 + z_3\alpha_3,
\end{aligned}$$

c'est-à-dire

$$\begin{vmatrix} x_1 - \lambda & y_1 & z_1 \\ x_2 & y_2 - \lambda & z_2 \\ x_3 & y_3 & z_3 - \lambda \end{vmatrix} = 0,$$

les x et y étant des nombres entiers rationnels λ satisfait à une équation du 3ᵉ degré dont tous les coefficients sont entiers, le coefficient du terme le plus élevé étant égal à 1, λ est un entier algébrique.

Soit maintenant β un nombre quelconque de l'idéal $\mathfrak{a}^{h_1}$, $\beta\alpha_1$, $\beta\alpha_2$, $\beta\alpha_3$ sont tous des nombres du produit idéal $(\lambda)\,\mathfrak{a}^m$. Si l'on représente ces trois nombres au moyen de la base $\lambda\alpha_1$, $\lambda\alpha_2$, $\lambda\alpha_3$ de

$(\lambda)\mathfrak{a}^m$ et que l'on élimine α_1, α_2, α_3 entre ces trois équations on obtient pour $\frac{\beta}{\lambda}$ une équation du troisième degré à coefficients entiers comme précédemment, c'est-à-dire que $\frac{\beta}{\lambda}$ est un nombre entier du corps.

Tout nombre de $\mathfrak{a}^{h_1}$ est divisible par λ, c'est-à-dire que $\mathfrak{a}^{h_1}$ est divisible par λ,

$$\mathfrak{a}^{h_1} = (\lambda)\mathfrak{j}.$$

On a donc

$$\mathfrak{a}^{m+h_1} = \mathfrak{a}^m \cdot \mathfrak{a}^{h_1} = \mathfrak{a}^m(\lambda)\mathfrak{j},$$

où $\mathfrak{j}$ est un idéal du corps.

L'équation idéale

$$\mathfrak{a}^{m+h_1} = (\lambda)\mathfrak{a}^m$$

donne de plus

$$\mathfrak{a}^m(\lambda)\mathfrak{j} = (\lambda)\mathfrak{a}^m,$$

ou comme on peut diviser par λ

$$\mathfrak{a}^m\mathfrak{j} = \mathfrak{a}^m,$$

d'où il résulte finalement que l'idéal $\mathfrak{j}$ contient aussi le nombre 1 (¹), c'est-à-dire que $\mathfrak{a}^{h_1} = (\lambda)$ est un idéal principal.

De l'équation

$$\mathfrak{a}^{h_1} = (\lambda) \sim 1$$

(¹) En effet tout nombre du produit $\mathfrak{a}^m\mathfrak{j}$ est un nombre de $\mathfrak{a}^m$ et réciproquement. Soit ι_1, ι_2, ι_3 la base de $\mathfrak{j}$, il est évident que tous les nombres de $\mathfrak{a}^m$ peuvent être mis sous la forme

$$\lambda_1\alpha_1(x_1\iota_1 + y_1\iota_2 + z_1\iota_3) + \lambda_2\alpha_2(x_2\iota_1 + y_2\iota_2 + z_2\iota_3) + \lambda_3\alpha_3(x_3\iota_1 + y_3\iota_2 + z_3\iota_3),$$

où λ_1, λ_2, λ_3 sont des entiers quelconques de $k(\vartheta)$ et x_i, y_i, z_i des entiers rationnels. Comme d'autre part

$$u_1\alpha_1 + u_2\alpha_2 + u_3\alpha_3$$

peuvent représenter tous les nombres de $\mathfrak{a}^m$, on peut déterminer les λ_i, x_i, y_i, z_i de telle sorte que $\lambda_i(x_i\iota_1 + y_i\iota_2 + z_i\iota_3)$ représentent pour $i = 1, 2, 3$ trois entiers rationnels premiers entre eux qui appartiennent à l'idéal $\mathfrak{j}$, et qui combinés linéairement entre eux d'une manière convenable au moyen de coefficients entiers rationnels donneront l'unité.

il résulte

$$\mathfrak{a}^{1+h_1} = \mathfrak{a}\cdot\mathfrak{a}^{h_1} \backsim \mathfrak{a}, \qquad \mathfrak{a}^{2+h_1} \backsim \mathfrak{a}^2, \text{ etc.,}$$

autrement dit il faut faire $m = 1$, et d'après l'hypothèse les idéaux $\mathfrak{a}, \mathfrak{a}^2, \ldots, \mathfrak{a}^{h_1-1}$ ne seront pas équivalents entre eux.

Soit alors $\mathfrak{a}$ un idéal non principal du corps $\mathfrak{b} = \mathfrak{a}^{h_1-1}$ est un autre idéal non principal ayant cette propriété que $\mathfrak{ab}$ est un idéal principal.

A l'aide de ce théorème nous pourrons en énoncer d'autres qu'il ne sera pas nécessaire de démontrer à nouveau.

Théorème. — Soient $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ trois idéaux différents de zéro, tels que

$$\mathfrak{ac} = \mathfrak{bc},$$

on a aussi

$$\mathfrak{a} = \mathfrak{b}.$$

On a aussi la réciproque d'un théorème précédent.

Théorème. — Si tous les nombres d'un idéal $\mathfrak{a}$ sont compris dans un idéal $\mathfrak{b}$, $\mathfrak{a}$ est divisible par $\mathfrak{b}$.

Et on peut encore dire que le plus grand commun diviseur de $\mathfrak{a}$ et de $\mathfrak{b}$ est l'idéal qui contient à la fois les nombres de $\mathfrak{a}$ et de $\mathfrak{b}$.

Enfin on a le

Théorème. — Lorsqu'un idéal premier $\mathfrak{p}$ divise le produit de deux facteurs il divise au moins l'un des facteurs.

Tous ces théorèmes réunis sont identiques au théorème qui dit : Tout idéal n'est décomposable que d'une seule manière en idéaux premiers.

En voici une conséquence importante : Tout idéal premier $\mathfrak{p}$ du corps divise un nombre premier rationnel.

En effet on peut déterminer un idéal $\mathfrak{j}$ tel que le produit $\mathfrak{p}\,.\,\mathfrak{j} = (\alpha)$ soit un idéal principal. Mais comme $(\alpha)(\alpha')(\alpha'') = a$ est un entier rationnel, $\mathfrak{p}$ divise a, et par suite un facteur premier p de a (et un seul).

En raisonnant maintenant comme au n° 16 nous verrions que le nombre h_1 tel que $\mathfrak{a}^{h_1}$ à un idéal principal est un diviseur du nombre h des classes.

La suite $\mathfrak{a}, \mathfrak{a}^2, \ldots, \mathfrak{a}^{h_1}$ s'appelle la période de l'idéal $\mathfrak{a}$.

Nous démontrerons le théorème suivant qui permet le calcul

numérique des idéaux de corps déterminés sans écrire un nombre illimité de nombres.

Théorème. — Il existe dans tout idéal non principal $\mathfrak{a}$ d'un corps $k(\vartheta)$ deux nombres α et α_1, tels que $\mathfrak{a}$ puisse être considéré comme le plus grand commun diviseur de (α) et de (α_1), c'est-à-dire qu'on puisse poser

$$\mathfrak{a} = (\alpha, \alpha_1).$$

Démonstration : Soit α un nombre de l'idéal $\mathfrak{a}$ tel que

$$(\alpha) = \mathfrak{a} \cdot \mathfrak{b},$$

où $\mathfrak{b}$ est premier avec $\mathfrak{a}$. On prendra dans $\mathfrak{a}$ un deuxième nombre α_1 qui n'est pas situé dans $\mathfrak{b}$ tel que

$$(\alpha_1) = \mathfrak{a} \cdot \mathfrak{c},$$

$\mathfrak{b}$ et $\mathfrak{c}$ seront nécessairement premiers entre eux, et l'on voit que $\mathfrak{a}$ est le plus grand commun diviseur de α et de α_1, c'est-à-dire

$$\mathfrak{a} = (\alpha, \alpha_1).$$

Car comme $\mathfrak{b}$ est premier avec $\mathfrak{c}$ on peut trouver dans $\mathfrak{b}$ un nombre β et dans $\mathfrak{c}$ un nombre γ tel que

$$\beta + \gamma = 1.$$

Tous les nombres α_i de $\mathfrak{a}$ peuvent être représentés par

$$\lambda\alpha + \lambda_1\alpha_1,$$

et en effet

$$\alpha_i = \alpha_i\beta + \alpha_i\gamma = \lambda\alpha + \lambda_1\alpha_1.$$

44. — La norme d'un idéal. — Nous dirons qu'un nombre α du corps $k(\vartheta)$ est congru à zéro, suivant le module $\mathfrak{j}$, ou que

$$\alpha \equiv 0 \ (\mathfrak{j}),$$

si α est contenu dans l'idéal $\mathfrak{j}$. Lorsque $\alpha \equiv 0 \ (\mathfrak{j})$, (α) est divisible par $\mathfrak{j}$. Deux entiers quelconques α et β sont dits congrus suivant le module $\mathfrak{j}$

$$\alpha \equiv \beta \ (\mathfrak{j})$$

lorsque leur différence appartient à l'idéal $\mathfrak{j}$.

Il résulte de la définition que deux nombres congrus à un troisième suivant le mod $\mathfrak{j}$ sont congrus entre eux. On peut répartir tous les entiers en groupes tels, que tous les nombres d'un même groupe soient congrus à un nombre donné suivant le module $\mathfrak{j}$. Tout nombre appartient à un groupe et à un seul, et tout nombre d'un groupe détermine ce groupe.

Si l'on prend un nombre dans chacune de ces classes on obtient un système de nombres entiers que nous désignerons par *système complet de restes* suivant le module $\mathfrak{j}$. Tout nombre du corps n'est congru qu'à un seul nombre de ce système de restes suivant le mod $\mathfrak{j}$.

Le choix des nombres d'un pareil système est arbitraire dans de certaines limites. Nous désignerons par $n(\mathfrak{j})$ le nombre des entiers contenus dans un système de restes complet, il prend le nom de *Norme* de l'idéal $\mathfrak{j}$.

Théorème. — Soit $\mathfrak{a}$ un idéal du corps dont la base est formée par

$$\begin{aligned}\alpha_1 &= a_{11}\omega_1 + a_{12}\omega_2 + a_{13}\omega_3\\ \alpha_2 &= a_{21}\omega_1 + a_{22}\omega_2 + a_{23}\omega_3\\ \alpha_3 &= a_{31}\omega_1 + a_{32}\omega_2 + a_{33}\omega_3,\end{aligned}$$

je dis que

$$n(\mathfrak{a}) = |(a_{11}a_{22}a_{33})|.$$

Démonstration : Au lieu de prendre pour base du corps une base quelconque, prenons d'abord comme base 1, ω^*, ω_1^* et exprimons les nombres de l'idéal au moyen de cette base, appliquons pour trouver la base de l'idéal le raisonnement que nous avons fait pour trouver la base du corps, nous verrons qu'on peut choisir comme base de l'idéal trois nombres de la forme

$$\begin{aligned}\alpha_1^* &= a\\ \alpha_2^* &= a_1 + a_2\omega^*\\ \alpha_3^* &= a_3 + a_4\omega^* + a_5\omega_1^*,\end{aligned}$$

où a est le plus petit nombre entier positif rationnel divisible par $\mathfrak{a}$ et où a_2, a_5 sont aussi des nombres entiers positifs.

On obtiendra des nombres incongrus mod $(\mathfrak{a})$ au moyen de

$$\beta = u + u_1\omega^* + u_2\omega_1^*$$

en donnant au coefficient u toutes les valeurs de 1 à a à u_1 les valeurs entières de 1 à a_2 à u_2 les valeurs entièrs de 1 à a_5.

Aucun de ces nombres n'est contenu dans $\mathfrak{a}$, deux d'entre eux ne peuvent être congrus suivant $\mathfrak{a}$, mais tout nombre est congru à un de ces nombres suivant $\mathfrak{a}$, c'est-à-dire que nous avons là un système complet de restes ([1]). Le nombre de ces restes est

$$a \,.\, a_2 \,.\, a_5.$$

On a

$$1 = u_{11}\omega_1 + u_{12}\omega_2 + u_{13}\omega_3$$
$$\omega^* = u_{21}\omega_1 + u_{22}\omega_2 + u_{23}\omega_3$$

de déterminant $(u_{11}u_{22}u_{33}) = \pm 1$.

On a

$$\alpha_i^* = b_{i1}\omega_1 + b_{i2}\omega_2 + b_{i3}\omega_3, \qquad (i = 1, 2, 3),$$

et

$$\begin{vmatrix} b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{23} \\ b_{31} & b_{32} & b_{33} \end{vmatrix} = \begin{vmatrix} u_{11} & u_{12} & u_{13} \\ u_{21} & u_{22} & u_{23} \\ u_{31} & u_{32} & u_{33} \end{vmatrix} \begin{vmatrix} a & 0 & 0 \\ a_1 & a_2 & 0 \\ a_3 & a_4 & a_5 \end{vmatrix} = \pm a \,.\, a_2 \,.\, a_5.$$

Enfin en exprimant α_1^*, α_2^*, α_3^* en fonction de α_1, α_2, α_3 suivant les formules

$$\alpha_i = v_{i1}\alpha_1^* + v_{i2}\alpha_2^* + v_{i3}\alpha_3^* \qquad \text{pour} \qquad (i = 1, 2, 3),$$

avec $(v_{11}, v_{22}, v_{33}) = \pm 1$, on a

$$\alpha_i = a_{i1}\omega_1 + a_{i2}\omega_2 + a_{i3}\omega_3$$

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = \begin{vmatrix} b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{23} \\ b_{31} & b_{32} & b_{33} \end{vmatrix} \cdot \begin{vmatrix} v_{11} & v_{12} & v_{13} \\ v_{21} & v_{22} & v_{23} \\ v_{31} & v_{32} & v_{33} \end{vmatrix} = \pm a a_2 a_5.$$

De sorte que dans tous les cas

$$n(\mathfrak{a}) = |\,(a_{11}a_{22}a_{33})\,|.$$

---

[1]) Le système des restes que l'on vient d'établir correspond au système des plus petits restes dans le domaine des nombres rationnels où 1, 2, ..., a forment un reste suivant a. On pourrait aussi transporter la notion de restes minima situés entre $-\frac{1}{2}a$ et $\frac{1}{2}a$ dans le domaine des nombres algébriques.

Le nombre $n(\mathfrak{a}) = aa_2a_3$ est un nombre de l'idéal $|n(\alpha)| = |\alpha\alpha'\alpha''|$, α étant un entier du corps représente aussi le nombre des entiers du corps incongrus suivant (α). Voir n° 12.

Théorème. — La norme d'un produit de deux idéaux $\mathfrak{a}$ et $\mathfrak{b}$ est égal au produit des normes des deux idéaux

$$n(\mathfrak{a} \cdot \mathfrak{b}) = n(\mathfrak{a}) \cdot n(\mathfrak{b}).$$

Démonstration : Soit α un entier du corps divisible par $\mathfrak{a}$ et tel que $\frac{(\alpha)}{\mathfrak{a}}$ soit premier avec $\mathfrak{b}$. Alors

$$\alpha\eta + \xi$$

représente des nombres incongrus mod $(\mathfrak{a}\mathfrak{b})$, si ξ parcourt un système complet incongru à $\mathfrak{a}$ et η un système complet de restes incongrus à $\mathfrak{b}$. Ce système contient $n(\mathfrak{a}) \cdot n(\mathfrak{b})$ nombres ; deux de ces nombres ne peuvent être congrus suivant le module $(\mathfrak{a}\mathfrak{b})$ et tout entier est congru à un de ces nombres suivant $(\mathfrak{a}\mathfrak{b})$. On a donc

$$n(\mathfrak{a}\mathfrak{b}) = n(\mathfrak{a}) \cdot n(\mathfrak{b}).$$

La norme d'un idéal appartient à l'idéal, à chaque idéal $\mathfrak{a}$ correspond donc un idéal $\bar{\mathfrak{a}}$ dit réciproque du premier, tel que

$$(n(\mathfrak{a})) = \mathfrak{a} \cdot \bar{\mathfrak{a}},$$

pour deux idéaux $\mathfrak{a}$, $\mathfrak{b}$ on a alors

$$n(\mathfrak{a}, \mathfrak{b}) = \mathfrak{a} \cdot \bar{\mathfrak{a}} \cdot \mathfrak{b} \cdot \bar{\mathfrak{b}}.$$

Appliquons le théorème qui vient d'être établi à un idéal premier.

Soit $\mathfrak{p}$ un idéal premier qui divise p, on a quatre cas possibles pour la base normale de p en employant les notations précédentes

$$p,\ a_1 + 1\omega^*, \qquad a_3 + a_2\omega^* + 1\omega_1^*,$$
$$p,\ a_1 + p\omega^*, \qquad a_3 + a_2\omega^* + 1\omega_1^*,$$
$$p,\ a_1 + 1\omega^*, \qquad a_3 + a_2\omega^* + p\omega_1^*,$$
$$p,\ a_1 + p\omega^*, \qquad a_3 + a_2\omega^* + p\omega_1^*,$$

c'est-à-dire que

$$n(\mathfrak{p}) = p^e \quad \text{ou} \quad e = 1, 2 \text{ ou } 3.$$

e est dit le degré de l'idéal premier $\mathfrak{p}$. On distingue donc des idéaux premiers du premier, second et troisième degré, et la norme d'un idéal premier $\mathfrak{p}$ est toujours une puissance p^e du nombre premier rationnel divisible par $\mathfrak{p}$.

Nous allons pouvoir établir les théorèmes qui permettent le calcul des classes d'idéaux d'un corps.

45. Les théorèmes de Minkowski qui permettent de déterminer les classes d'idéaux. — *Lemme.* Tout idéal $\mathfrak{a}$ du corps $k(\vartheta)$ contient un nombre α tel que

$$|n(\alpha)| \leq |n(\mathfrak{a})\sqrt{d}|.$$

Démonstration : Soit $k(\vartheta)$ un corps réel et $\alpha_1, \alpha_2, \alpha_3$ la base de l'idéal $\mathfrak{a}$ sous la forme

$$\alpha_i = a_{i1}\omega_1 + a_{i2}\omega_2 + a_{i3}\omega_3 \qquad (i = 1, 2, 3).$$

D'après le théorème de Minkowski on peut déterminer trois entiers rationnels non nuls x, y, z tels que les valeurs absolues de

$$\begin{aligned} f_1 &= \alpha_1 x + \alpha_2 y + \alpha_3 z \\ f_2 &= \alpha_1' x + \alpha_2' y + \alpha_3' z \\ f_3 &= \alpha_1'' x + \alpha_2'' y + \alpha_3'' z \end{aligned}$$

soient respectivement $\leq \varkappa_1$, $\leq \varkappa_2$, $\leq \varkappa_3$. $\varkappa_1, \varkappa_2, \varkappa_3$ désignant trois nombres dont le produit est égal au déterminant des formes f_1, f_2, f_3.

$$\varkappa_1\varkappa_2\varkappa_3 = |(\alpha_1\alpha_2'\alpha_3'')| = |(a_{11}a_{22}a_{33})\sqrt{d}|.$$

Si donc on pose $f_1 = \alpha$, $f_2 = \alpha'$, $f_3 = \alpha''$, α est un nombre de $\mathfrak{a}$ tel que

$$|n(\alpha)| \leq \varkappa_1\varkappa_2\varkappa_3$$

ou

$$|n(\alpha)| \leq |n(\mathfrak{a})\sqrt{d}|.$$

Si $k(\vartheta)$ est un corps imaginaire $k(\vartheta')$ étant le corps imaginaire conjugué et $k(\vartheta'')$ le corps réel conjugué nous poserons

$$f_1 = \frac{1}{\sqrt{2}}\{(\alpha_1 + \alpha_1')x + (\alpha_2 + \alpha_2')y + (\alpha_3 + \alpha_3')z\},$$

$$f_2 = \frac{1}{\sqrt{-2}}\{(\alpha_1 - \alpha_1')x + (\alpha_2 - \alpha_2')y + (\alpha_3 - \alpha_3')z\}.$$

On fera $z_1 = z_2$, on voit comme précédemment que le théorème est vrai pour les corps imaginaires car

$$\text{comme} \quad f_1^2 + f_2^2 = (f_1 + \sqrt{-1}\, f_2)(f_1 - \sqrt{-1}\, f_2)$$

$$\frac{f_1^2 + f_2^2}{2} = (\alpha_1 x + \alpha_2 y + \alpha_3 z)(\alpha_1' x + \alpha_2' y + \alpha_3' z).$$

Nous allons pouvoir démontrer le théorème fondamental.

Théorème. — Toute classe d'idéal contient au moins un idéal dont la norme est plus petite en valeur absolue que la racine carrée du déterminant du corps.

Démonstration : Soit $\mathfrak{a}$ un idéal du corps $k(\vartheta)$ est $\bar{\mathfrak{a}}$ un idéal tel que

$$(\alpha) = \mathfrak{a} . \bar{\mathfrak{a}}.$$

Il existe dans $\bar{\mathfrak{a}}$ un nombre $\bar{\alpha}$ tel que

$$n(\bar{\alpha}) \leqq n(\bar{\mathfrak{a}}) \, |\sqrt{d}\,|.$$

$\bar{\alpha}$ est divisible par $\mathfrak{a}$, c'est-à-dire

$$\bar{\alpha} = \bar{\mathfrak{a}} . \mathfrak{a}_1,$$
$$n(\bar{\mathfrak{a}}\mathfrak{a}_1) = n(\bar{\alpha}) \leqq n(\bar{\mathfrak{a}}) \, |\sqrt{d}\,|,$$

par suite aussi

$$n(\mathfrak{a}_1) \leqq |\sqrt{d}\,|.$$

Comme $(\alpha) = \mathfrak{a}\bar{\mathfrak{a}}$ et que $(\bar{\alpha}) = \bar{\mathfrak{a}}\mathfrak{a}_1$ il s'ensuit que $\mathfrak{a}$ est équivalent à $\mathfrak{a}_1$ avec la propriété $n(\mathfrak{a}_1) \leqq |\sqrt{d}\,|$.

Pour trouver le nombre des classes d'un corps quelconque $k(\vartheta)$ d'une façon directe, il suffit donc de décomposer en facteurs les nombres premiers rationnels positifs $\leqq |\sqrt{d}\,|$ et de voir quels sont parmi ces facteurs ceux qui sont équivalents.

46. Le calcul des idéaux premiers dans le corps $k(\vartheta)$. — Soit un corps déterminé par le nombre ϑ, racine de l'équation irréductible

$$G(x) = x^3 + a_1 x^2 + a^2 x + a_3 = 0.$$

Il s'agit de trouver les idéaux premiers $\mathfrak{p}, \mathfrak{p}_1$, etc., facteurs du nombre premier rationnel p.

Nous supposerons d'abord que p ne divise pas $d(z)$, c'est-à-dire soit

$$d(z) \not\equiv 0 \ (p).$$

On a vu que tout idéal peut être considéré comme le plus grand diviseur de deux nombres du corps

$$\mathfrak{p} = (p, \alpha),$$

α étant un entier du corps. Si l'on suppose que p ne divise pas $d(z)$ on peut mettre α sous la forme

$$a + bz + cz^2,$$

a, b, c étant entiers, comme nous allons le voir.

Nous avons vu que la base d'un corps peut être mise sous la forme

$$\omega = 1, \quad \omega_1 = \frac{-A + a_1 + z}{D}, \quad \omega_2 = \frac{A^2 - a_1 A + a_2 + Az + z^2}{D^2 D_1}$$

où D^2 et D_1 sont des diviseurs déterminés de $d(z)$.

On peut donc écrire pour tout entier α

$$\alpha = \frac{a + bz + cz^2}{D^2 D_1}.$$

Soit maintenant $\mathfrak{p}$ le plus grand commun diviseur de p et de α, il sera aussi le plus grand commun diviseur de p et de $D^2D_1\alpha$, car comme p ne divise ni D ni D_1 $\mathfrak{p}$ est premier avec D^2D_1. Il reste à distinguer deux cas, suivant que $D^2D_1\alpha$ est du premier ou du second degré en z

$$\mathfrak{p} = (p, a + bz),$$
$$\mathfrak{p} = (p, a + bz + cz^2).$$

Soit d'abord

(1) $$\mathfrak{p} = (p, a + bz),$$

où b est premier avec p. Comme l'idéal renferme en outre toute combinaison linéaire à coefficients entiers de p et de α, c'est-à-dire les nombres

(2) $$x \cdot pz + y(a + bz),$$

il renferme aussi un nombre de la forme $-A+z$ (où A est un entier rationnel) car on peut toujours déterminer x et y de façon que

$$px+by=1.$$

Alors

$$\mathfrak{p}=(p, -A+z),$$

car de p et de $-A+z$ on peut toujours déduire par des combinaisons linéaires (avec des nombres premiers à p)

$$a+bz.$$

Il ne reste qu'à déterminer A, pour cela multiplions $-A+z$ par

$$(-A+z')(-A+z'')$$

qui appartient au corps, nous obtenons

$$-A^3-a_1A^2-a_2A-a_3,$$

c'est-à-dire un entier rationnel différent de zéro qui doit être divisible par p. A est donc une solution de la congruence

(3) $$x^3+a_1x^2+a_2x+a_3\equiv 0\ (p).$$

Si cette congruence n'est pas possible p n'a certainement pas de diviseur de la forme (1).

Deuxièmement, soit

$$\mathfrak{p}=(p, a+bz+cz^2),$$

et supposons c premier avec p ; on verra comme précédemment qu'il est permis de faire $c=1$, c'est-à-dire que

(4) $$\mathfrak{p}=(p, a+bz+z^2),$$

et p ne contient des nombres de la forme a_1+b_1z' que si a_1, b_1 sont tous deux divisibles par p ; sans quoi $\mathfrak{p}$ se ramènerait à la forme (1).

Multiplions $a+bz+cz^2$ par $z+z$ où z est encore indéterminé, en vertu de

$$z^3+a_1z^2+a_2z+a_3=0$$

on a

$$\mathfrak{p} = (p, a + b\mathfrak{z} + \mathfrak{z}^2, az + (a+b)z\mathfrak{z} + (b+z)\mathfrak{z}^2 + \mathfrak{z}^3, a_3 + a_2\mathfrak{z} + a_1\mathfrak{z}^2 + \mathfrak{z}^3, \ldots)$$
$$= (p, a + b\mathfrak{z} + \mathfrak{z}^2, az - a_3 + (a + bz - a_2)\mathfrak{z} + (b + z - a_1)\mathfrak{z}^2, \ldots).$$

Déterminons z de façon que

$$b - a_1 + z \equiv 0 \ (p).$$

On voit d'après la remarque que nous avons faite à propos des idéaux de la forme $a_1 + b_1\mathfrak{z}$ que

$$a + bz - a_2 \equiv 0 \ (p),$$
$$az - a_3 \equiv 0 \ (p),$$

il en résulte que

$$(5) \qquad (a + b\mathfrak{z} + c\mathfrak{z}^2)(z - \mathfrak{z}) \equiv a_3 + a_2\mathfrak{z} + a_1\mathfrak{z}^2 + \mathfrak{z}^3 \ (p).$$

On obtient par conséquent a, b, $a + b\mathfrak{z} - c\mathfrak{z}^2$ lorsqu'on décompose suivant le module p, $a_3 + a_2\mathfrak{z} + a_1\mathfrak{z}^2 + \mathfrak{z}^3$ en un produit d'un facteur linéaire et d'un facteur du second degré.

La recherche des idéaux qui divisent un nombre premier p est ramenée à la recherche des racines de la congruence

$$(6) \qquad x^3 + a_1x^2 + a_2x + a_3 \equiv 0 \ (p).$$

Rappelons les théorèmes relatifs à cette congruence.

1. Si A est une racine de la congruence (6) on a, suivant p

$$x^3 - a_1x^2 + a_2x - a_3 \equiv (x - A) f_1(x) \equiv 0 \ (p),$$

où $f_1(x)$ est une fonction entière du second degré.

2. La congruence (6) ne peut avoir plus de 3 racines distinctes.

Comme la décomposition de (p) en idéaux premiers n'est possible que d'une seule manière, nous pouvons formuler les théorèmes suivants :

I. Si la congruence (6) n'a pas de solution, (p) ne peut être décomposé dans le corps, c'est un idéal du troisième degré.

II. Si la congruence (6) n'a qu'une seule solution $x = A$, on a

$$(7) \qquad x^3 + a_1x^2 + a_2x + a_3 \equiv (x - A)(x^2 + bx + a) \ (p),$$

(p) est divisible par

(8) $\mathfrak{p} = (p, -A + z), \qquad \mathfrak{p}_1 = (p, a + bz + cz^2),$

$\mathfrak{p}, \mathfrak{p}_1$ sont des idéaux du premier et du second degré, et on a

$$(p) = \mathfrak{p} \cdot \mathfrak{p}_1.$$

III. Si la congruence (6) a trois racines A_1, A_2, A_3, c'est-à-dire si

(9) $x^3 + a_1x^2 + a_2x + a_3 \equiv (x - A_1)(x - A_2)(x - A_3)\ (p),$

p est divisible par trois idéaux du premier degré

$$\mathfrak{p}_i = (p, -A_i + z) \qquad (i = 1, 2, 3),$$

et on a

(10) $(p) = \mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdot \mathfrak{p}_3.$

Supposons maintenant que p est un diviseur de $d(z)$. La question devient beaucoup plus difficile. Il nous suffira d'indiquer les résultats, quant aux démonstrations nous renvoyons le lecteur aux auteurs indiqués plus loin.

Nous ferons cependant les considérations suivantes :

Lorsque $d(z) \equiv 0\ (p)$, la congruence

$$x^3 + a_1x^2 + a_2x + a_3 \equiv 0\ (p)$$

a une racine multiple $x = A_1$, on a ou bien

$$x^3 + a_1x^2 + a_2x + a_3 \equiv (x - A_1)^2 (x - A_2)\ (p)$$

ou bien

$$x^3 + a_1x^2 + a_2x + a_3 \equiv (x - A_1)^3\ (p).$$

Car si

$$G'(x) = 3x^2 + 2a_1x + a^2$$

est la dérivée de $G(x)$ la condition nécessaire et suffisante pour que

$$G(x) \equiv 0\ (p) \qquad \text{et} \qquad G'(x) \equiv 0$$

aient une racine commune est $d(z) \equiv 0\ (p)$ comme on peut le voir par l'élimination de x.

Soit A la racine commune de

$$G(x) \equiv 0 \qquad \text{et} \qquad G'(x) \equiv 0 \ (p),$$

et soit

$$G(x) \equiv (x - A) f_1(x) \ (p),$$
$$G'(x) \equiv f_1(x) + (x - A) f_1'(x) \ (p).$$

D'après cela on voit que $G'(x)$ ne peut être divisible par $x - A$ suivant le module p, que si

$$f_1(x) \equiv (x - A) f_2(x) \ (p),$$

c'est-à-dire que $G(x) \equiv 0 \ (p)$ a une racine double

$$G(x) \equiv (x - A)^2 f_2(x) \ (p).$$

On pourrait croire que p est alors divisible par le carré d'un idéal premier, ce n'est pas toujours vrai. On a le théorème énoncé par Dedekind et démontré par Hensel [1] :

Théorème. — Tous les nombres premiers et ceux-là seulement qui divisent le discriminant d du corps, sont divisibles par le carré d'un idéal premier.

Nous avons su démontrer facilement ce théorème dans le cas du corps quadratique et nous pouvions soupçonner ce résultat. Il faut entendre que si p divise d il contient $\mathfrak{p}^2$ ou $\mathfrak{p}^3$.

Pour démontrer ce théorème et en général pour décomposer les facteurs premiers contenus dans $d(ʒ)$, il faut prendre

$$\mathfrak{p} = (p,\ a\omega + b\omega_1 + c\omega_2,\ \ldots),$$

en considérant u, u_1, u_2 comme des variables on pose

$$\xi = u\omega + u_1\omega_1 + u_2\omega_2,$$

---

[1] R. DEDEKIND. — *Ueber den Zusammenhang der Theorie der Ideale und der höheren Kongruenzen. Abhand. der math. Klasse der kg'. Gesellschaft der Wissenchaften zu Göttingen.*, 23 Band., 1878. Une démonstration toute différente est due à K. HENSEL, *Untersuchung der Fundamentalgleichung einer Gattung für eine reelle Primzahl als Modul und Intersuchung der Teiler der Diskriminante*, Crelles Journ., 113, Bd., 1894.

Voir HILBERT. — *Zahlbericht*, chap. IV.

Voir encre HENSEL. — *Jahresber, d. d. Math. Ver.*, Bd. 6, und Gött. Nachr., 1897, Crelles Journal, 127, 128, 129.

et on donne à cette forme des variables u, u_1, u_2 le nom de forme fondamentale du corps, elle satisfait à une équation du troisième degré

$$F = (x - \xi)(x - \xi')(x - \xi'') = x^3 + U_1 x^2 + U_2 x + U_3 = 0$$

dite équation fondamentale.

Soient trois fonctions à coefficients entiers rationnels

$$F_i(x, u, u_1, u_2) \quad \text{pour} \quad i = 1, 2, 3,$$

telles que

$$F_1 \equiv F_2 + F_3 \ (p),$$

quels que soient x, u, u_1, u_2 on dit que F_1 *est décomposable* suivant le module p ou que F_1 est divisible par F_2 et F_3 suivant le module p.

Si d'autre part F_1 n'est divisible que par une autre fonction congrue elle-même à $F_1(p)$ ou à un nombre rationnel suivant (p) on dit que F_1 est une fonction première suivant p.

On a alors les théorèmes suivants pris textuellement dans le traité de M. Hilbert.

I. Si $\mathfrak{p}$ est un idéal premier de degré f contenu dans p il y a toujours une fonction $P(x, u, u_1, u_2)$ de degré f en x, telle que si on remplace x par ξ elle ait les propriétés suivantes :

Les coefficients des puissances et des produits de u, u_1, u_2 sont tous divisibles par $\mathfrak{p}$ et ne le sont pas tous par $\mathfrak{p}^2$, et ils ne sont pas divisibles non plus par un idéal différent de $\mathfrak{p}$ contenu dans p.

II. Si

$$(p) = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\mathfrak{p}_3^{e_3},$$

on a

$$F \equiv P_1^{e_1}P_2^{e_2}P_3^{e_3} \ (p),$$

où P_1, P_2, P_3 sont des fonctions premières distinctes suivant p de x, u, u_1, u_2 et de plus si on pose

$$F = P_1^{e_1}P_2^{e_2}P_3^{e_3} + p\Phi,$$

Φ est une fonction entière à coefficients entiers rationnels de x, u, u_1, u_2 qui n'est divisible suivant p par aucune des fonctions premières P_1, P_2, P_3.

Le théorème II en particulier renferme tous les éléments nécessaires pour décomposer un nombre premier p.

Par exemple $\mathfrak{p}_1$ contient les nombres que l'on obtient en remplaçant x par la forme fondamentale ξ dans P_1. D'ailleurs il n'est nécessaire d'appliquer le théorème dans toute sa généralité que si p est contenu dans $\frac{d(z)}{d}$, car on a le

Théorème. — Soit z défini par

$$G(x) \equiv x^3 + a_1 x^2 + a_2 x + a_3 = 0$$

et p un nombre premier rationnel tel que $\frac{d(z)}{d} \not\equiv 0\ (p)$, toute décomposition de $G(x)$ suivant le module p

$$G(x) \equiv G_1(x)^{r_1} G_2(x)^{r_2} G_3(x)^{r_3}\ (p)$$

nous donne la décomposition de p en idéaux premiers du corps z sous la forme

$$(p) = (p, G_1(z))^{r_1} (p, G_2(z))^{r_2} (p, G_3(z))^{r_3}.$$

On trouve de nombreuses applications numériques des développements de ce chapitre dans la « Göttinger Dissertation de L.-W. Reid ». Nous y puiserons les exemples suivants :

1er *Exemple.* — z racine de

$$x^3 + x + 1 = 0,$$

$d(z) = -31$ et aussi $d = -31$. On peut donc prendre pour base $1, z, z^2$. Pour déterminer le nombre des classes il faut décomposer 2, 3 et 5.

Comme ces nombres sont premiers avec d, il suffit de décomposer

$$x^3 + x + 1 \equiv 0$$

suivant les modules 2, 3 et 5. On trouve que 2 et 5 ne se décomposent pas, tandis que

$$3 = (-z + 1)(z^2 - z + 2).$$

On a donc $h = 1$. On trouve les unités

$$z \quad \text{et} \quad z + 1.$$

2e *Exemple.* — z est racine de

$$x^3 + 6x + 8 = 0,$$

$d(z) = -2592 = -2^5 . 3^4$. On peut prendre pour base $1, z, \frac{z^2}{2}$, il en résulte $d = -2^3 . 3^4$, il vient

$$(2) = \left(2, 1 + z + \frac{z^2}{2}\right)^2 \left(2, \frac{z^2}{2}\right),$$

$$(3) = (3, z - 1)^3,$$

$$(5) = (5, z - 1)(5, 2 + z + z^2),$$

$$(7) = (7, z - 2)(7, 3 + 2z + z^2).$$

Ces idéaux se répartissent en trois classes. On trouve enfin comme unité $z + 1$.

3e *Exemple.* — $x^3 - 8x + 4 = 0$.

$d(z) = -1616 = 2^4 . 101$. On peut prendre comme base $1, z, \frac{z^2}{2}$, d'où $d = 2^2 . 101$. Il vient

$$2 = \left(\frac{z^2}{2}\right)^3 (132 z^2 + 68 z - 1023),$$

$$3 = (z - 1)(z^2 + z - 7).$$

Le nombre des classes $h = 1$ et

$$2z - 1, \qquad 132 z^2 + 68 z - 1023$$

sont parmi les unités.

47. Les unités du corps $k(z)$. — Parmi les nombres il en est d'une importance particulière, ceux dont la norme est ± 1 et que l'on désigne par le nom : *unités* du corps.

Soit ε un pareil nombre, c'est-à-dire

$$\varepsilon\varepsilon'\varepsilon'' = \pm 1,$$

il en résulte d'abord que $\frac{1}{\varepsilon}$ est un entier du corps, car

$$\varepsilon'\varepsilon'' = \frac{\pm 1}{\varepsilon},$$

et $\varepsilon'\varepsilon''$ est un entier du corps $k(z)$.

Il est évident que ± 1 sont les unités les plus simples. De plus si ε est une unité du corps, tout nombre $\pm \varepsilon^e$ où e est un exposant entier positif ou négatif est aussi une unité, car

$$\varepsilon^e \varepsilon'^e \varepsilon''^e = (\varepsilon \varepsilon' \varepsilon'')^e = \pm 1.$$

Dans le cas où le corps $k(\vartheta)$ est réel ainsi que tous ses conjugués, ε ne peut être une racine de l'unité ± 1, en tant que ces racines sont imaginaires. Si $k(\vartheta)$ est réel et si $k(\vartheta')$, $k(\vartheta'')$ sont imaginaires on ne peut encore avoir comme unité du corps d'autre racine de 1 que ± 1.

En effet, supposons par exemple que

$$\eta' = \frac{a\vartheta'^2 + b\vartheta' + c}{N}$$

soit une racine imaginaire de l'unité dans $k(\vartheta')$.

Les nombres conjugués η'' et η seraient aussi des racines de l'unité, mais alors on aurait $\eta = \pm 1$ et on aurait, en coefficients entiers et rationnels a, b, c l'équation

$$a\vartheta^2 + b\vartheta + c = \pm N.$$

Mais comme par définition ϑ satisfait à

$$\vartheta^3 + a_1\vartheta^2 + a_2\vartheta + a_3 = 0,$$

ϑ, racine commune à ces deux équations serait un nombre rationnel, ce qui est contraire à notre hypothèse. Il faut donc que $a = 0$, $b = 0$, $c = \pm N$ et par suite $\eta' = \pm 1$.

On voit de même que toute unité ε est du corps telle que $|\varepsilon| = 1$ est égale à ± 1, car si ε est réel $|\varepsilon| = 1$ exige $\varepsilon = \pm 1$. Si ε est imaginaire $|\varepsilon| = 1$ nous donne $|\varepsilon'| = |\varepsilon| = 1$ $|\varepsilon''| = 1$ d'où l'unité réelle $\varepsilon'' = \pm 1$ ainsi que ε et ε'.

Ceci posé nous démontrerons le

Théorème (¹). — Dans tout corps (réel ou imaginaire) $k(\vartheta)$ du troisième degré il existe une unité différente de ± 1.

(¹) P.-G. Lejeune-Dirichlet. — *Œuvres*, t. I, p. 642. Parties du théorème général, *ibid.*, p. 662 et pour des nombres cubiques, p. 632.

H. Minkowski. — *Géom. der Zahlen*, Nr. 44, p. 137.

D. Hilbert. — *Bericht*, chap. VI, §§ 19 et 20.

La démonstration de ce théorème diffère peu de celle que nous avons donnée pour le corps quadratique. Nous abrégerons donc quelque peu.

Démonstration : I. — Supposons d'abord le discriminant d du corps positif, c'est-à-dire que les trois corps $k(\vartheta)$, $k(\vartheta')$, $k(\vartheta'')$ sont réels. Soient A, A_1, A_2 trois nombres réels positifs quelconques dont le produit

$$(1) \qquad A \cdot A_1 \cdot A_2 = |\sqrt{d}|.$$

On démontre grâce au théorème de Minkowski qu'on peut toujours trouver un nombre α dans $k(\vartheta)$ tel que

$$(2) \qquad |\alpha| \leqq A, \qquad |\alpha'| \leqq A_1, \qquad |\alpha''| < A_2,$$

comme α est un entier du corps on a

$$|\alpha\alpha'\alpha''| \geqq 1,$$

et par suite

$$\alpha \geqq \frac{1}{|\alpha'\alpha''|},$$

et par conséquent

$$|\alpha| \geqq \frac{1}{A_1 A_2} \quad \text{ou} \quad |\alpha| \geqq \frac{A}{|\sqrt{d}|}.$$

On a donc pour α et ses conjugués

$$(3) \qquad \begin{cases} A \geqq \alpha \geqq \dfrac{A}{|\sqrt{d}|}, \\ A_1 \geqq \alpha' \geqq \dfrac{A_1}{|\sqrt{d}|}, \\ A_2 \geqq \alpha'' \geqq \dfrac{A_2}{|\sqrt{d}|}. \end{cases}$$

On pourrait écrire la dernière

$$\frac{\sqrt{d}}{A \cdot A_1} \geqq |\alpha''| \geqq \frac{1}{A \cdot A_1}.$$

Choisissons dès lors trois nombres

$$B = \frac{A}{|\sqrt{d}|}, \qquad B_1 = \frac{A_1}{|\sqrt{d}|}, \qquad B_2 = \frac{A_2\,|\sqrt{d}|^3}{|\sqrt{d}|},$$

dont le produit

$$BB_1B_2 = |\sqrt{d}|.$$

Il y a dans $k(\vartheta)$ un entier β tel que

$$(4) \quad \begin{cases} B \geq |\beta| > \dfrac{B}{|\sqrt{d}|}, \\ B_1 \geq |\beta'| \geq \dfrac{B_1}{|\sqrt{d}|}, \\ B_2 \geq |\beta''| \geq \dfrac{B_2}{|\sqrt{d}|}, \end{cases}$$

où la dernière peut s'écrire

$$\frac{|\sqrt{d}|}{BB_1} \geq |\beta''| \geq \frac{1}{BB_1},$$

posons à nouveau

$$C = \frac{B}{|\sqrt{d}|}, \qquad C_1 = \frac{B_1}{|\sqrt{d}|}, \qquad C_2 = \frac{B_2}{|\sqrt{d}|},$$

et déterminons un nombre γ comme nous avons déterminé β. Comme le discriminant $|d| > 1$ on voit que les nombres $|\alpha|$, $|\beta|$, ..., ainsi $|\alpha'|$, $|\beta'|$ forment une suite décroissante car les inégalités précédentes peuvent s'écrire

$$A \geq |\alpha| \geq \frac{A}{|\sqrt{d}|} \geq |\beta| \geq \frac{A}{|\sqrt{d^2}|} \geq |\gamma| \geq \frac{A}{|\sqrt{d^3}|} \geq \delta \ldots.$$

Tandis qu'on verrait de même que les $|\alpha''|$, $|\beta''|$, ... forment une suite croissante.

Utilisons maintenant ce fait que les idéaux principaux (α), (β), (γ), ... forment une suite illimitée d'idéaux de normes $\leqq |\sqrt{d}|$ et remarquant qu'il n'y a qu'un nombre limité d'idéaux dont la norme est plus petite qu'un nombre donné.

La suite (α), (β), (γ), ... contient un nombre infini d'idéaux égaux entre eux.

Soit $(\alpha) = (\gamma)$ et $|\alpha| > |\gamma|$, le quotient $\varepsilon = \dfrac{\alpha}{\gamma}$ représentera une unité différente de ± 1.

Les inégalités nous montrent que

$$|\varepsilon| > 1, \qquad |\varepsilon'| > 1, \qquad |\varepsilon''| < 1$$

si l'on pose

$$\varepsilon' = \frac{\alpha'}{\gamma'_1}, \qquad \varepsilon'' = \frac{\alpha''}{\gamma''_1}.$$

On voit d'ailleurs que (ε) ne peut être égal à (ε').

On voit de même qu'on peut obtenir une unité telle que

$$|\eta| > 1, \qquad |\eta'| < 1, \qquad |\eta''| > 1.$$

II. — Supposons d négatif. Supposons $k(\vartheta)$ réel tandis que $k(\vartheta')$ $k(\vartheta'')$ sont imaginaires, et choisissons A, A_1 réels et positifs tels que $AA_1^2 = |\sqrt{d}|$, on peut alors déterminer α de façon que

$$(2a) \qquad |\alpha| \leqq A, \qquad |\alpha'| \leqq A_1,$$

et par suite

$$|\alpha''| \leqq A_1.$$

On a alors

$$(3a) \quad \begin{cases} A \geqq |\alpha| \geqq \dfrac{A}{|\sqrt{d}|}, \\ A_1 \geqq |\alpha'| \geqq \dfrac{A_1}{|\sqrt{d}|}. \end{cases}$$

On pose

$$B = \frac{A}{|\sqrt{d}|}, \qquad B_1 = A_1 |\sqrt{d}|.$$

de telle sorte que

$$BB_1^2 = |\sqrt{d}|,$$

et on construit β de $k(\vartheta)$ tel que

$$|\beta| \leqq B, \qquad |\beta'| = |\beta''| \leqq B_1.$$

En répétant le raisonnement précédent on trouve une unité ε de $k(\vartheta)$ différente de ± 1 et ε', ε'' dans $k(\vartheta')$ et $k(\vartheta'')$.

Si

$$|\varepsilon| > 1, \qquad |\varepsilon'| = |\varepsilon''| < 1$$

ou

$$|\eta| < 1, \qquad |\eta'| = |\eta''| > 1.$$

Nous pouvons énoncer le théorème de Dirichlet que nous met-

tons sous une forme permettant de l'appliquer à un corps quelconque.

Théorème. — Si parmi les trois corps conjugués $k(\vartheta)$, $k(\vartheta')$, $k(\vartheta'')$ il y a r_1 corps réels et $r_2 = \frac{3 - r_1}{2}$ couples de corps conjugués imaginaires, il y a dans chacun des trois corps $r_1 + r_2 - 1 = r$ unités fondamentales telles que toute autre unité ξ du corps puisse se montrer d'une seule façon sous la forme

$$\xi = \pm \varepsilon_1^{e_1} \dots \varepsilon_r^{e_r},$$

où $e_1, \dots e_2$ désignent des exposants rationnels positifs ou négatifs.

On a deux cas possibles, $r_1 = 1$, $r_2 = 1$, il y a alors une unité fondamentale.

Ou bien $r_1 = 3$, $r_2 = 0$ et il y a deux unités fondamentales.

Le dernier cas est le plus difficile, M. Minkowski d'abord et M. Hilbert ensuite l'ont démontré complètement. Nous donnerons ici la démonstration de M. Minkowski.

Démonstration : Soient $k(\vartheta)$, $k(\vartheta')$, $k(\vartheta'')$ les trois corps, nous avons vu qu'il y a deux unités ε, η telles que nous avons le droit d'admettre

$$|\varepsilon| > 1, \qquad |\varepsilon'| > 1, \qquad |\varepsilon''| < 1.$$
$$|\eta| > 1. \qquad |\eta'| < 1, \qquad |\eta''| > 1.$$

Si ξ est un nombre quelconque du corps, les valeurs réelles $\log|\xi|$, $\log|\xi'|$, $\log|\xi''|$ sont dites les logarithmes du nombre ξ, nous les écrirons

$$l(\xi) = \log|\xi|, \qquad l_1(\xi) = \log|\xi'|, \qquad l_2(\xi) = \log|\xi''|,$$

et comme $\xi\xi'\xi'' = \pm 1$, si ξ est une unité les logarithmes d'une unité satisfont à

$$(1) \qquad f = l(\xi) + l_1(\xi) + l_2(\xi) = 0,$$

et d'autre part toute *unité du corps* sera une solution de l'équation $f = 0$.

Dans le cas où l'un des logarithmes, ou tous les trois logarithmes, sont nuls ξ est nécessairement égal à ± 1. Donc, trouver les unités du corps cela revient à résoudre l'équation $f = 0$ pour des valeurs des logarithmes, toutes différentes de zéro.

Posons

$$(2)\qquad f_2(\xi) = hl(\xi) + h_1 l_1(\xi),$$

et déterminons h et h_1 de façon que

$$f_2(\eta) = hl(\eta) + h_1 l_1(\eta) > 0.$$

On peut prendre par exemple

$$h_1 = -l(\varepsilon) \qquad \text{et} \qquad h = l_1(\varepsilon),$$

car $l_1(\eta)$ est négatif puisque $|\eta'| < 1$, tandis que $l(\varepsilon)$, $l_1(\varepsilon)$, $l(\eta)$ sont positifs.

On peut mettre toute solution de l'équation (1) sous la forme

$$(3)\qquad \begin{cases} l(\xi) = s_1 l(\varepsilon) + s_2 l(\eta), \\ l_1(\xi) = s_1 l_1(\varepsilon) + s_2 l_1(\eta), \\ l_2(\xi) = s_1 l_2(\varepsilon) + s_2 l_2(\eta). \end{cases}$$

où s_1, s_2 sont des valeurs numériques réelles quelconques.

Ces expressions satisfont identiquement l'égalité (1) et pour tout système de valeurs donné $l(\xi)$, $l_1(\xi)$, $l_2(\xi)$ on peut calculer s_1, s_2, et cela d'une seule manière car $f_2(\eta) > 0$.

Pour $\xi = \varepsilon$, (3) nous donne $s_1 = 1$, $s_2 = 0$,

$$\xi = \eta, \qquad s_1 = 0, \qquad s_2 = 1.$$

Nous allons montrer maintenant qu'il n'y a qu'un nombre fini d'unités pour lesquelles

$$(4)\qquad 0 \leqq s_1 \leqq 1, \qquad 0 \leqq s_2 \leqq 1.$$

Si cette condition est remplie pour l'unité ξ on a

$$|l(\xi)| \leqq |l(\varepsilon)| + |l(\eta)|,$$
$$|l_i(\xi)| \leqq |l_i(\varepsilon)| + |l_i(\eta)|, \qquad (i = 1, 2),$$

c'est-à-dire que les valeurs absolues $|\xi|$, $|\xi'|$, $|\xi''|$, sont inférieures à des nombres finis dépendant uniquement de ε et de η. Soit

$$\xi = x + y\omega_1 + z\omega_2$$

un entier du corps, calculons x, y, z par les équations

$$\begin{aligned} x + \omega_1 y + \omega_2 z &= \xi, \\ x + \omega_1' y + \omega_2' z &= \xi', \\ x + \omega_1'' y + \omega_2'' z &= \xi''. \end{aligned}$$

nous obtenons $x = \lambda_1\xi + \lambda_2\xi' + \lambda_3\xi''$ et des valeurs analogues pour y et z. Si les $|\xi|$ sont inférieurs à une limite déterminée il en sera de même de $|x|$, $|y|$, $|z|$.

Il en résulte que l'on ne peut prendre pour x, y, z qu'un nombre limité de valeurs telles que $|\xi|$, $|\xi'|$, $|\xi''|$ soient inférieurs à une limite déterminée.

Nous pouvons répartir toutes les valeurs de ξ représentées par (3) et telles que

$$0 \leqq s_1 < 1, \qquad 0 \leqq s_2 < 1$$

en deux classes.

La première contient les unités pour lesquelles $s_2 = 0$, la seconde celles pour lesquelles $s_2 > 0$. Alors nous déterminerons dans la première classe l'unité ε_1 pour laquelle s_1 a sa plus petite valeur S_1 différente de zéro ; et dans la seconde une unité ε_2 pour laquelle s_2 prend sa plus petite valeur S_2.

Il n'y a alors aucune unité à part ± 1 pouvant se mettre sous la forme (3) et satisfaisant à

$$(5) \qquad 0 \leqq s_1 < S_1, \qquad 0 \leqq s_2 < S_2.$$

Désignons par ξ une unité du corps et par e_1, e_2 deux nombres entiers rationnels positifs ou négatifs du corps que nous supposons indéterminés $\frac{\xi}{\varepsilon_1^{e_1}\varepsilon_2^{e_2}}$ est aussi une unité du corps dont les logarithmes sont

$$\begin{aligned} L &= l(\xi) - e_1 l(\varepsilon_1) - e_2 l(\varepsilon_2), \\ L_1 &= l_1(\xi) - e_1 l_1(\varepsilon_1) - e_2 l_1(\varepsilon_2), \\ \text{et } L_2 & \end{aligned}$$

on a

$$l(\varepsilon_1) = S_1 l(\varepsilon) \qquad \text{et} \qquad l(\varepsilon_2) = S' l(\varepsilon) + S_2 l(\eta).$$

et si l'on veut représenter L_1, L_2 suivant (3) on trouve

$$s_1 = \frac{l_1(\xi)\,l(\eta) - l(\xi)\,l_1(\eta)}{f_2(\eta)} - e_1 S_1 - e_2 S,$$

$$s_2 = \frac{-\,l_1(\xi)\,l(\eta) + l(\xi)\,l_1(\eta)}{f_2(\eta)} - e_2 S_2.$$

Comme $f_2(\eta)$ est positif la dernière équation nous permet de déterminer pour e_2 et ensuite la première pour e_1 des valeurs entières rationnelles positives ou négatives telles que s_1, s_2 satisfassent aux inégalités (5).

Il faut alors

$$L = 0, \qquad L_1 = 0,$$

et par suite $L_2 = 0$ ou encore

$$\frac{\xi}{\varepsilon_1^{e_1}\varepsilon_2^{e_2}} = \pm 1, \qquad \xi = \pm\, \varepsilon_1^{e_1}\varepsilon_2^{e_2}.$$

Le théorème de Dirichlet est démontré lorsque les trois corps sont réels.

Le second cas où $d < 0$ et $k(\vartheta)$ désigne un corps réel et où $k(\vartheta')$, $k(\vartheta'')$ sont des corps conjugués imaginaires ne nécessite pas une démonstration particulière.

Car si ε_1 est l'unité de $k(\vartheta)$ qui a la plus petite valeur absolue parmi les unités dont la valeur absolue est > 1, on démontre comme pour le corps quadratique que toute unité ξ du corps est de la forme

$$\xi = \pm\, \varepsilon_1^{e_1},$$

où e_1 est un nombre entier rationnel positif ou négatif.

Le théorème de Dirichlet est démontré pour le corps cubique.

CHAPITRE V

—

LE CORPS RELATIF

La théorie des corps algébriques a pour but d'étudier les propriétés des nombres algébriques entiers satisfaisant à une équation irréductible de degré m.

Nous en avons examiné les deux cas les plus simples, nous ne pousserons pas plus loin. Mais nous allons exposer une autre généralisation de la théorie des nombres en ses principes fondamentaux, car là nous retrouverons un nouveau champ d'exploration fructueux, et ces notions ont trouvé d'importantes applications dans des problèmes considérables de l'algèbre et de la théorie des fonctions.

Elles se rattachent aux théorèmes de réciprocité.

Aux nos 24 et 25 nous avons obtenu la loi de réciprocité quadratique pour des nombres premiers rationnels

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

avec les théorèmes complémentaires en nous basant sur ce fait que l'on peut superposer au domaine des nombres entiers un corps de nombres $k(\sqrt{p})$ ou $k(\sqrt{\pm q})$ dont les propriétés nous fournissent les lois de réciprocité.

Puisqu'on peut étendre l'étude des congruences aux nombres et aux idéaux d'un corps, on peut se demander si les lois de réciprocité vraies pour les solutions des congruences de nombres ordinaires ne s'étendent pas aux nombres et aux idéaux d'un corps.

Lorsqu'on se limite aux congruences quadratiques, c'est-à-dire à

une généralisation des lois de réciprocité quadratique on a un critère pour la généralisation de nos considérations [1].

Pour développer logiquement la méthode qui nous a permis de démontrer la formule

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}},$$

on essaiera de construire sur le corps quadratique un nouveau quadratique le « *corps quadratique relatif* » pour déduire des propriétés de ce corps relatif la loi cherchée. En effet cet effort a été couronné de succès. M. Hilbert [2] a démontré ainsi la loi de réciprocité pour un nombre assez vaste de corps de base [3]. Nous prendrons comme exemple le corps quadratique relatif à un corps de base quadratique et nous citerons des exemples numériques.

48. — Notions fondamentales. Définitions. — Soit le corps quadratique $k(\sqrt{m})$ où m entier rationnel ne contient pas de facteur au carré. Soit μ un nombre quelconque du corps différent de o et de 1 et qui n'est pas le carré d'un nombre entier du corps, de plus soient α et β deux nombres quelconques du corps $k(\sqrt{m})$ entiers ou fractionnaires. Alors tous les nombres

$$(1) \qquad \alpha + \beta\sqrt{\mu}$$

forment un domaine K ou un corps de nombre dans le sens indiqué précédemment, car la somme, le produit, la différence et le quotient de deux nombres de la forme (1) est encore un nombre de cette forme.

Tout nombre $A = \alpha + \beta\sqrt{\mu}$ de ce domaine satisfait à une équation du second degré de la forme

$$X^2 - 2\alpha X + \alpha^2 - \beta^2\mu = 0,$$

(1) Gauss a traité le cas le plus simple pour le corps $k(\sqrt{-1})$, *Œuvres*, t. II, p. 130. *Theoria resid. biquad.*, Comm II, n° 60 (56-60) et *œuvres*, t. II. p. 172.

(2) Hilbert. — *Ueber die Theorie des relativquadratischen Zahlkörpers. Math. Annal.*, t. LI, pp. 1-127.

H. Dörrie a étudié un cas particulier, dans sa dissertation « *Das quadratische Reziprozitätsgesetz im quadratischen Zahlkörper mit der Klassenanzahl* 1. » Göttingen, 1898. Il y prend comme exemple le corps $k(\sqrt{-3})$.

(3) Furtwängler. — *Abh. und Nachr. von der kg. Ges der Wiss. zu Göttingen* et aussi *Math. Ann.*, t. LXIII.

dont les coefficients appartiennent au corps $k(\sqrt{m})$; aussi on dit que le corps K *est un corps relatif quadratique* par rapport à $k(\sqrt{m})$. K est dit un *corps relatif* ou un *sur-corps* par rapport à k ; et comme d'autre part K contient tous les nombres de k, k est dit aussi un *sous-corps* de K. Le corps K est superposé au corps k comme k est superposé au domaine des nombres rationnels.

Désormais nous désignerons les nombres du corps relatif par des majuscules grecques, et les nombres du sous-corps au corps de base comme jusqu'alors par des petites lettres grecques. Ici encore elles ne désigneront que des nombres *entiers* que nous définirons plus loin.

Deux nombres $\alpha + \beta\sqrt{\mu}$, $\alpha - \beta\sqrt{\mu}$ qui ne diffèrent que par le signe de $\sqrt{\mu}$ sont dits *relativement* conjugués, et on a coutume de dire que la seconde résulte de la première par la substitution $S(\sqrt{\mu} : -\sqrt{\mu})$. Nous écrirons deux nombres relativement conjugués A et S(A). De plus A et $s(A)$ seront deux nombres obtenus en changeant dans l'un d'eux $\sqrt{m}$ en $-\sqrt{m}$, c'est-à-dire par la substitution $s(\sqrt{m} : -\sqrt{m})$.

Un nombre quelconque de K satisfait une équation du 4e degré à coefficients rationnels. Par conséquent, d'une façon absolue K est un cas particulier du corps du 4e degré. Tous les nombres A de ce corps peuvent s'exprimer rationnellement en fonction de

$$B = \sqrt{\mu} + \sqrt{m}$$

sous la forme

$$A = a + a_1 B + a_2 B^2 + a_3 B^3,$$

où a, a_1, a_2, a_3 sont des nombres rationnels qui peuvent être fractionnaires.

A est une racine de l'équation du 4e degré

$$(x - A)(x - s(A))(x - S(A))(x - Ss(A)) = 0.$$

Un nombre A est un nombre entier du corps relatif lorsqu'il est racine d'une équation de la forme

$$x^2 + \alpha x + \beta = 0,$$

où α et β sont des entiers de $k(\sqrt{m})$, c'est-à-dire que A est racine d'une équation du quatrième degré à coefficients entiers rationnels de la forme

$$x^4 + a_1 x^3 + a_2 x^2 + a_3 x + a_4 = 0,$$

ou encore que **A** est un nombre entier dans le corps du quatrième degré K.

On peut aussi dire **A** est entier si

$$\mathbf{A} + S(\mathbf{A}) \quad \text{et} \quad \mathbf{A}.S(\mathbf{A})$$

sont des entiers du sous-corps.

Le produit du nombre relativement conjugué **A** . $S(\mathbf{A})$ est dit la *norme relative* de **A**, nous la désignerons par $N_k(\mathbf{A})$. La norme relative d'un entier **A** de K est un entier du corps de base $k(\sqrt{m})$.

La norme relative d'un nombre α du sous-corps k est $N_k(\alpha) = \alpha^2$ car $S(\alpha) = \alpha$.

On déduit tout d'abord de cette définition que tout nombre de K compris dans $k(\sqrt{m})$ est un entier de ce dernier corps, et que tout entier de K qui est rationnel est un entier rationnel.

On démontre comme pour les corps cubiques (n° 39).

Théorème. — La somme, la différence, le produit de deux entiers de K est un entier de K [1].

La différence

$$\Delta_k = \mathbf{A} - S(\mathbf{A})$$

qui est dite la différente relative est entière si **A** est entier.

$$D_k(\mathbf{A}) = (\mathbf{A} - S(\mathbf{A}))^2$$

est dit le discriminant relatif de A.

Et on voit que le discriminant relatif est la norme relative de la différente relative

$$D_k(\mathbf{A}) = - N_k(\Delta_k).$$

49. Les bases du corps relatif. — Tout nombre du corps $k(\sqrt{\mu})$ peut être représenté sous la forme

$$\frac{\alpha + \beta\sqrt{\mu}}{\gamma}.$$

Voyons s'il n'existe pas dans K une infinité de systèmes de quatre nombres tels, que tout nombre entier de K soit une com-

[1] Voir Hilbert. — *Bericht*, chap. v et chap. xv.

binaison linéaire à coefficients entiers et rationnels de ces quatre nombres.

Nous remarquerons d'abord que les entiers de K sont de deux sortes : 1° les entiers de K qui ne sont pas des entiers de k ; 2° ceux qui sont des entiers de k.

Ces derniers peuvent être mis sous la forme $x + y\omega$, où x, y sont des entiers rationnels et 1, ω une base de k. Il nous suffit donc de nous occuper des nombres

$$\frac{\alpha + \beta\sqrt{\mu}}{\gamma},$$

où $\beta \neq 0$.

Lorsque α, β, γ n'ont pas de facteur idéal commun inutile, un raisonnement analogue à celui du n° 6 nous montre que le numérateur γ d'un entier ne peut admettre comme facteurs premiers : 1° que des facteurs idéaux contenus au carré au moins dans μ ; 2° des facteurs premiers de 2.

Lorsque le corps de base a un nombre de classes $h = 1$, γ ne contient pas d'autres facteurs premiers que ceux que l'on vient d'énumérer, mais si $h > 1$ il faut supposer α, β, γ divisibles par un certain idéal accessoire.

Soit $\bar{a}$ et $\bar{e}$ les plus grands entiers contenus dans $\frac{a}{2}$ et $\frac{e}{2}$, c'est-à-dire $\bar{a} = \left[\frac{a}{2}\right]$ et $\bar{e} = \left[\frac{e}{2}\right]$, on a les deux théorèmes suivants, que l'on peut démontrer d'après le schéma du n° 6.

1er *Théorème.* — Le corps de base $k(\sqrt{m})$ a une classe $h = 1$, le nombre 2 est divisible par les facteurs premiers λ_1, λ_2 élevé aux puissances l_1, l_2, $2 = \lambda_1^{l_1}\lambda_2^{l_2}$; de plus soit

$$\mu = \lambda_1^{a_1}\lambda_2^{a_2}\pi_1^{e_1}\ldots\pi_r^{e_r},$$

et l'un des exposants au moins a ou e est impair.

Soient $g_1 \leqq l_1$, $g_2 \leqq l_2$ les plus grands exposants positifs pour lesquels

$$\mu \equiv \nu^2 \ (\lambda_1^{2g_1 - a}\lambda_2^{2g_2 - a_2})$$

peut être satisfaite par un nombre entier ν du corps de base et si ν

est une solution de cette congruence, telle que l'on puisse poser ([1])

$$\nu = \pi_1^{c_1} \dots \pi_r^{c_r} \nu_1,$$

$$\Omega = \frac{\nu + \sqrt{\mu}}{\lambda_1^{g_1+a_1} \lambda_2^{g_2+a_2} \pi_1^{c_1} \dots \pi_r^{c_r}} = \frac{\nu + \sqrt{\mu}}{\gamma}$$

est un entier du corps $K(\sqrt{\mu})$ et les quatre nombres

$$1, \quad \omega, \quad \Omega, \quad \omega\Omega$$

forment une base du corps relatif.

Donc, avec l'hypothèse $h = 1$, tout entier du corps peut être mis sous la forme

$$\frac{\alpha + \beta\sqrt{\mu}}{\gamma},$$

où γ a le sens indiqué et où α, β sont des entiers de k. Il est à remarquer que g_1 et $g_2 > 0$ que si a_1, a_2 sont pairs, et que ν est nécessairement divisible par $\lambda_1^{a_1}\lambda_2^{a_2}$. Si $g_1 = g_2 = 0$, Ω est de la forme $\frac{\sqrt{\mu}}{\gamma}$.

2e *Théorème.* — Le corps de base $k(\sqrt{m})$ a un nombre de classes $h > 1$ et on a

$$(2) = \mathfrak{l}_1^{l_1}\mathfrak{l}_2^{l_2},$$

$$(\mu) = \mathfrak{l}_1^{a_1}\mathfrak{l}_2^{a_2}\mathfrak{p}_1^{c_1} \dots \mathfrak{p}_r^{c_r}.$$

Si la congruence

$$\mu \equiv \nu^2, \quad (\mathfrak{l}_1^{2(g_1+a_1)}\mathfrak{l}_2^{2(g_2+a_2)})$$

peut être satisfaite par un entier du corps de base et si $\mathfrak{d} = (\beta_1, \beta_2)$ est un idéal premier avec $\mathfrak{l}_1$ et $\mathfrak{l}_2$ et tel que

$$\mathfrak{l}_1^{g_1+a_1}\mathfrak{l}_2^{g_2+a_2}\mathfrak{p}_1^{c_1} \dots \mathfrak{p}_r^{c_r}\mathfrak{d} = (\gamma)$$

soit un idéal principal, si de plus on choisit ν (ce qui est possible

([1]) Cette hypothèse est permise ; car si ν est un nombre entier on peut toujours déterminer ν_1 tel que

$$\nu \equiv \pi_1^{c_1} \dots \pi_r^{c_r}\nu_1, \quad (\lambda_1^{2(g_1+a_1)}\lambda_2^{2(g_2+a_2)}) \quad \text{car} \quad \pi_1, \dots, \pi_r$$

sont premiers avec 2.

d'après les théorèmes sur les congruences linéaires) de telle sorte que

$$(\nu) = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r} . \mathfrak{n},$$

les nombres

$$\Omega_1 = \beta_1 \frac{\nu + \sqrt{\mu}}{\gamma}, \qquad \Omega_2 = \beta_2 \frac{\nu + \sqrt{\mu}}{\gamma}$$

sont des entiers du corps $K(\sqrt{\mu})$ et les quatre nombres

$$1, \quad \omega, \quad \Omega_1, \quad \Omega_2$$

forment une base du corps relatif.

D'après ce théorème le choix de γ est encore arbitraire dans de certaines limites suivant le choix de $\mathfrak{b}$; cependant tout nombre du corps peut se ramener à un autre ayant le dénominateur γ. Soit

$$\Omega = \beta \frac{\sigma + \sqrt{\mu}}{\gamma_1}$$

où

$$\frac{\gamma}{\gamma_2} = \frac{\mathfrak{b}}{\mathfrak{b}_1}.$$

Si l'on multiplie le numérateur et le dénominateur de Ω par $\frac{\mathfrak{b}}{\mathfrak{b}_1}$ on a

$$\Omega = \frac{\rho + \tau\sqrt{\mu}}{\gamma_1 \frac{\mathfrak{b}}{\mathfrak{b}_1}} = \frac{\rho + \tau\sqrt{\mu}}{\gamma},$$

car β d'après la façon dont il a été obtenu est divisible par $\mathfrak{b}_1$.

De toute base on déduit une infinité de systèmes de quatre nombres qui forment également une base, deux de ces systèmes se déduisent l'un de l'autre par une substitution unité.

A la suite du deuxième théorème nous ferons remarquer que l'idéal $\mathfrak{b}$ peut aussi être choisi de façon à ne contenir que les idéaux $\mathfrak{l}_1, \mathfrak{l}_2, \dots \mathfrak{p}_1, \dots \mathfrak{p}_r$ comme facteurs premiers, de façon que γ soit contenu dans 4μ. Le second théorème contient le premier comme cas particulier ; nous les avons cités séparément parce que le premier se comprend immédiatement.

50. Les idéaux du corps relatif. — La définition des idéaux

s'applique au corps K. Tout idéal $\mathfrak{j} = (\iota, \iota_1)$ du sous-corps est aussi un idéal $\mathfrak{J}$ du corps relatif. Mais il est évident que tout idéal $\mathfrak{J}$ du corps relatif n'est pas nécessairement un idéal du corps de base.

La définition d'un idéal principal reste la même.

Lorsqu'on fait subir à tous les nombres d'un idéal la substitution $S(\sqrt{\mu} : -\sqrt{\mu})$ on obtient un nouvel idéal que l'on désigne par $S(\mathfrak{J})$ et qui se dit l'idéal relativement conjugué de $\mathfrak{J}$. Un idéal $\mathfrak{J}$ qui est égal à son conjugué relatif et ne contient aucun idéal de k en facteur est dit un idéal ambige.

On peut exprimer tous les nombres d'un idéal au moyen d'une base $1, \omega, \Omega_1, \Omega_2$ et répéter les raisonnements que nous avons faits pour établir la base d'un idéal, on trouve alors que

$$\mathfrak{J} = (i, \iota, \mathrm{I}, \mathrm{I}_1),$$

où $i, \iota, \mathrm{I}, \mathrm{I}_1$ représentent la base de l'idéal.

En ce qui concerne les définitions du produit de deux idéaux, de la norme d'un idéal et la démonstration de la décomposition d'un idéal en facteurs il suffit de se reporter aux n[os] 11, 43, 44.

Soit $n(\mathfrak{j})$ la norme d'un idéal $\mathfrak{j}$ de k et dans ce corps k lui-même, soit de plus $N(\mathfrak{j})$ la norme du même idéal dans le corps supérieur

$$N(\mathfrak{j}) = n(\mathfrak{j})^2.$$

Car si

$$\mathfrak{j} = (i, i_0 + i_1\omega)$$

est un idéal de k, une base de ce même idéal dans K est

$$i, \quad i_0 + i_1\omega, \quad a_1 + b_1\omega + \frac{i}{g}\Omega_1, \quad a_2 + b_2\omega + ci_1\Omega_1 + gi_1\Omega_2,$$

par suite

$$N(\mathfrak{j}) = (ii_1)^2 = n(\mathfrak{j})^2.$$

Si par exemple (nous rencontrerons ce cas un peu plus loin) $\mathfrak{P}$ est un idéal de $K(\sqrt{\mu})$ tel que $\mathfrak{P}^2 = \mathfrak{p}$,

$$(n(\mathfrak{p}))^2 = N(\mathfrak{p}) = N(\mathfrak{P}^2) = N(\mathfrak{P})^2,$$

et comme $n(\mathfrak{p})$ et $N(\mathfrak{P})$ sont des entiers positifs

$$n(\mathfrak{p}) = N(\mathfrak{P}).$$

On généralise aussi l'idée de norme et on considère *la norme relative d'un idéal* $\mathfrak{J}$, on entend par là le produit

$$N_k(\mathfrak{J}) = \mathfrak{J} \cdot S(\mathfrak{J}).$$

La norme relative d'un idéal $\mathfrak{J}$ de k est toujours un idéal du corps de base.

En effet, soit

$$\mathfrak{J} = (i, i_1, I, I_1)$$

un idéal du corps relatif représenté par sa base. Réunissons tous les nombres de l'idéal $\mathfrak{J} \cdot S(\mathfrak{J})$ qui sont dans le corps de base et formons un idéal $\mathfrak{j}$ qui soit situé dans le corps de base,

$$\mathfrak{j} = (i^2, ii_1, i_1^2, IS(I), I_1S(I_1), ISI_1 + I_1SI, II_1S(I_1I_2) \ldots),$$

$\mathfrak{j}$ sera identique à $\mathfrak{J} \cdot S(\mathfrak{J})$.

Car comme

(1) $$IS(I_1) + I_1S(I) \equiv 0 \ (\mathfrak{j}),$$

(2) $$IS(I) \cdot I_1S(I_1) \equiv 0 \ (\mathfrak{j}^2),$$

on a aussi

$$IS(I_1) \equiv 0 \ (\mathfrak{j}) \quad \text{et} \quad I_1S(I) \equiv 0 \ (\mathfrak{j}).$$

Car si $\mathfrak{P}$ divise $\mathfrak{j}$ en étant premier avec $IS(I_1)$ la congruence (1) nous apprend qu'il est premier aussi avec $I_1S(I)$ par conséquent $I \cdot S(I_1)I_1S(I)$ ne pourrait être divisible par $(\mathfrak{P}^2)$ comme l'exige la congruence (2). Il en résulte de même que $iS(I)$, iI, etc. sont divisibles par $\mathfrak{j}$ ou encore $\mathfrak{j} = N_k(\mathfrak{J})$ comme nous l'avons annoncé.

Il en résulte en particulier que le carré de tout idéal ambige est un idéal de k.

Remarque. — (Au lieu de procéder comme aux n°s 13 et 143 pour démontrer que la décomposition des idéaux n'est possible que d'une seule manière on pourrait tirer parti de ce que le carré d'un idéal ambige est toujours un idéal du corps de base ; et appliquer les théorèmes démontrés pour ce corps de base).

Nous définirons encore la *différente relative du corps de k*, c'est

$$\mathfrak{D}_k = (A - S(A), A_1 - S(A_1) \ldots)$$

le plus grand commun diviseur des différentes relatives des entiers du corps, et le discriminant relatif du corps

$$\mathfrak{d} = \mathfrak{D}_k^2 = (A - S(A), A_1 - S(A_1) \ldots)^2.$$

La différente relative est un idéal de K, le discriminant relatif est un idéal du corps de base, car

$$\mathfrak{d} = N_k(\mathfrak{D}_k).$$

51. Les facteurs du discriminant relatif. — *Théorème.* — Soit $\mathfrak{p}$ un idéal du corps de base qui ne divise pas (2) et tel que $\mathfrak{p}^e$ soit contenu dans μ, le discriminant relatif du corps supérieur $K(\sqrt{\mu})$ n'est divisible par $\mathfrak{p}$ que si e est impair.

De plus si dans $k(\sqrt{m})$ on a

$$(2) = \mathfrak{l}_1^{r_1}\mathfrak{l}_2^{r_2}$$

et si $\mathfrak{l}_i$ est contenu dans μ, à la puissance a_i le discriminant relatif de $K(\sqrt{u})$ est premier avec $\mathfrak{l}_i$ s'il existe dans le corps de base un nombre ν tel que

$$\mu \equiv \nu^2, (\mathfrak{l}_i^{2r_i + a_i}),$$

et dans ce cas-là seulement [1].

Démonstration : Le discriminant relatif

$$\mathfrak{d} = (A - S(A), A_1 - S(A_1) \ldots)^2.$$

Si on y exprime A_i en fonction de la base

$$\mathfrak{d} = \left(\frac{2\beta_1\sqrt{\mu}}{\gamma}, \quad \frac{2\beta_2\sqrt{\mu}}{\gamma}, \quad \frac{2(x\beta_1 + y\beta_2)\sqrt{\mu}}{\gamma}, \ldots\right)^2$$

ou

$$\mathfrak{d}(\gamma^2) = (\mu) 2^2(\beta_1, \beta_2)^2 = (\mu)(2)^2\mathfrak{b}^2,$$

ou en remplaçant par les facteurs premiers

$$\mathfrak{d} = \frac{\mathfrak{l}_1^{a_1}\mathfrak{l}_2^{a_2}\mathfrak{p}^{e_1}\ldots\mathfrak{p}_2^{e_2}\mathfrak{l}_1^{2r_1}\mathfrak{l}_2^{2r_2}\mathfrak{b}^2}{\mathfrak{l}_1^{2g_1+2a_1}\mathfrak{l}_2^{2g_2+2a_2}\mathfrak{p}_1^{2e_1}\ldots\mathfrak{p}^{2e}\mathfrak{b}^2},$$

d'où résulte immédiatement le théorème.

---

(1) Voir Hilbert. — *Math. Ann.*, t. LI, p. 5.

Si e_i est pair $\frac{e_i}{2} = \bar{e}_i$, $\mathfrak{d}$ est premier avec $\mathfrak{p}_i$; si e_i est impair $e = 2\bar{e}_i + 1$, $\mathfrak{d}$ contient $\mathfrak{p}_i^1$.

De plus si on a

$$\mu \equiv \nu^2, (\mathfrak{l}_i^{2l_i + a_i}),$$

il faut que a_i soit pair et dans l'expression de γ trouvée au n° 49 il faut faire $g_i = l_i$.

Alors le numérateur et le dénominateur de $\mathfrak{d}$ contiennent $\mathfrak{l}_i^{2l_i + a_i}$, et $\mathfrak{d}$ est premier avec $\mathfrak{l}_i$. Tandis que si a_i est impair ou si

$$\mu \equiv \nu^2, (\mathfrak{l}_i^{2g_i + a_i})$$

n'est satisfaite que pour $g_i < l_i$, $\mathfrak{d}$ contient nécessairement $\mathfrak{l}_i$ et la deuxième partie du théorème est démontrée.

En réunissant les résultats pour $\mathfrak{l}_1$ et $\mathfrak{l}_2$ on déduit :

Théorème. — Si (μ) est premier avec (2) et si on a

$$\mu \equiv \nu^2, (2^2),$$

le discriminant relatif $\mathfrak{d}$ du corps $K(\sqrt{\mu})$ est premier avec (2).

52. — Les idéaux premiers du corps relatif. — Pour reconnaître si un idéal premier $\mathfrak{p}$ du corps de base se décompose dans le corps relatif K on applique les théorèmes suivants (Hilbert, *l. c.*, p. 8):

1er *Théorème.* — Soit $\mathfrak{p}$ un idéal premier du corps k qui ne divise ni 2 ni μ, $\mathfrak{p}$ n'est le produit de deux idéaux $\mathfrak{P}$, $\mathfrak{P}_1$ du corps relatif que si μ est reste quadratique suivant $\mathfrak{p}$, c'est-à-dire s'il existe dans k un nombre α tel que

$$\mu \equiv \alpha^2 \ (\mathfrak{p}),$$

et dans ce cas seulement.

Démonstration : Si

$$\mu \equiv \alpha^2 \ (\mathfrak{p}),$$

posons

$$\mathfrak{P} = (\mathfrak{p}, \alpha + \sqrt{\mu}), \qquad \mathfrak{P}_1 = S(\mathfrak{P}) = (\mathfrak{p}, \alpha - \sqrt{\mu}),$$

alors $\mathfrak{P}$ et $S(\mathfrak{P})$ sont différents, car en vertu de l'hypothèse α est premier avec $\mathfrak{p}$, et par suite

$$(\mathfrak{p}, \alpha + \sqrt{\mu}, \alpha - \sqrt{\mu}, 2\alpha, 2\sqrt{\mu}, 2\mu) = (1)$$

De plus on a pour $\mathfrak{p}$

$$\mathfrak{p} = \mathfrak{P} . S(\mathfrak{P}) = (\mathfrak{p}^2, \mathfrak{p}(\alpha + \sqrt{\mu}), \mathfrak{p}(\alpha - \sqrt{\mu}), \mu - \alpha^2, 2\mathfrak{p}\alpha, 2\mathfrak{p}\mu, \mathfrak{p} \ldots),$$

ce qui démontre une partie du théorème.

Réciproquement, soit $\mathfrak{p}$ un idéal du corps k, qui se décompose dans le corps relatif suivant

$$\mathfrak{p} = \mathfrak{P} \cdot \mathfrak{P}_1,$$

l'égalité des normes relatives des deux membres nous donne

$$\mathfrak{p}^2 = \mathfrak{P} S(\mathfrak{P}) \cdot \mathfrak{P}_1 S(\mathfrak{P}_1),$$

et par suite

$$\mathfrak{P}_1 = S(\mathfrak{P}),$$

puisque la décomposition n'est possible que d'une seule manière. Soit alors **A** un nombre de $\mathfrak{P}$ qui appartient au corps relatif, on a

$$N_k(\mathbf{A}) \equiv 0 \ (\mathfrak{p}),$$

soit

$$\mathbf{A} = \frac{\alpha + \beta\sqrt{\mu}}{\gamma}, \qquad N_k(\alpha + \beta\sqrt{\mu}) \equiv 0 \ (\mathfrak{p}).$$

Supposons d'abord que (γ) ne soit pas divisible par $\mathfrak{p}$. Si on avait $\beta \equiv 0 \ (\mathfrak{p})$ au aurait aussi $\alpha \equiv 0 \ (\mathfrak{p})$ et α et β appartiendraient à $\mathfrak{p}$, nous pouvons faire abstraction de ce cas. Si β est premier avec $\mathfrak{p}$, il y a, nous le savons, un nombre ξ de k tel que

$$\beta\xi \equiv \pm 1 \ (\mathfrak{p}),$$

et ξ est premier avec $\mathfrak{p}$, c'est pourquoi

$$\alpha^2 - \beta^2\mu \equiv 0 \ (\mathfrak{p})$$

ce qui nous donne

$$(\xi\alpha)^2 - \mu \equiv 0 \ (\mathfrak{p}),$$

μ est reste quadratique de $\mathfrak{p}$. Dans le cas où $\mathfrak{p}$ divise γ mais où il est premier avec β le raisonnement subsiste. Si γ est divisible par $\mathfrak{p}^{e_1}$ et que α et β contiennent $\mathfrak{p}^e$ avec $e_1 \geqq e$, soit $\mathfrak{s}$ un idéal premier avec $\mathfrak{p}^e$ et équivalent à $\mathfrak{p}^e$, $\frac{\mathfrak{p}^e}{\mathfrak{s}} = \frac{\pi}{\sigma}$ où π est divisible exac–

tement par $\mathfrak{p}$. On pose $\alpha = \frac{\pi}{\sigma}\alpha^*$, $\beta = \frac{\pi}{\sigma}\beta^*$, alors α^* et β^* sont premiers avec $\mathfrak{p}$ et on a

$$\alpha^{*2} - \beta^{*2}\mu \equiv 0 \ (\mathfrak{p}).$$

Le théorème est démontré.

En procédant de la même manière et en employant la base établie pour le corps relatif on voit :

2ᵉ *Théorème.* — Soit $\mathfrak{l}_i$ un idéal premier du corps $k(\sqrt{m})$ dont la puissance $\mathfrak{l}_i^{e}$ᵉᵐᵉ divise 2, supposons μ premier avec $\mathfrak{l}_i$ et congru à un nombre de k suivant $\mathfrak{l}_i^{2e}$, de façon que le discriminant relatif du corps $K(\sqrt{\mu})$ soit premier avec $\mathfrak{l}_i$, la condition nécessaire et suffisante pour que $\mathfrak{l}_i$ se décompose en deux idéaux premiers est qu'il existe un nombre α de k satisfaisant à

$$\mu \equiv \alpha^2 \ (\mathfrak{l}_i^{2e+1}).$$

Ces théorèmes permettent de se prononcer pour des idéaux qui ne divisent pas le discriminant relatif.

Nous compléterons par les théorèmes suivants :

3ᵉ *Théorème.* — La différente relative du corps $K(\sqrt{\mu})$ est divisible par tous les idéaux premiers qui sont ambiges et par ceux-là seulement.

Démonstration : La différente relative $\mathfrak{D}_k$ est un idéal qui est égal à son conjugué relatif et ne peut être divisible que par des idéaux premiers ambiges ou certains idéaux de premiers k, car si l'on pose

$$\mathfrak{D}_k = \mathfrak{P} \,.\, \mathfrak{P}_1 \ldots \mathfrak{P}_r,$$

$\mathfrak{P} \,.\, \mathfrak{P}_1 \ldots \mathfrak{P}_r$ sont des idéaux de K, on a aussi

$$\mathfrak{D}_k = S(\mathfrak{P})S(\mathfrak{P}_1) \ldots S(\mathfrak{P}_r) \quad \text{car} \quad \mathfrak{D}_k = S(\mathfrak{D}_k).$$

Il faut donc

$$\mathfrak{P} = S(\mathfrak{P}) \quad \text{ou} \quad \mathfrak{P} = S(\mathfrak{P}_i).$$

Si donc deux idéaux $\mathfrak{P}_a$ et $S(\mathfrak{P}_a)$ étaient différents $\mathfrak{D}$ serait divisible par $\mathfrak{P}_a S(\mathfrak{P}_a)$.

Mais

$$\mathfrak{P}_a S(\mathfrak{P}_a) = N_k(\mathfrak{P}_a) = \mathfrak{p}$$

est un idéal du corps de base et ne peut diviser $\mathfrak{D}_k$ si $\mathfrak{p}$ est différent

de $\mathfrak{l}_1$ et de $\mathfrak{l}_2$, c'est-à-dire si $\mathfrak{p}$ est premier avec 2. Car le discriminant relatif

$$\mathfrak{d} = \mathfrak{D}_k^2 = (\mathrm{A} - S(\mathrm{A}), \mathrm{A}_1 - S(\mathrm{A}_1), \ldots)^2$$

ne peut contenir outre des facteurs de 2 que des idéaux $\mathfrak{p}$ du corps de base qui entrent dans μ à une puissance impaire et alors $\mathfrak{p}$ est contenu avec l'exposant (1) dans $\mathfrak{d}$. Si donc $\mathfrak{D}_k$ était divisible par un idéal premier $\mathfrak{p}^2$, $\mathfrak{d} = \mathfrak{D}_k^2$ serait divisible par $\mathfrak{p}^2$ ce qui est impossible.

D'autre part si le discriminant relatif $\mathfrak{d}$ contient un idéal $\mathfrak{l}_i$ qui divise 2, on peut démontrer facilement que $\mathfrak{l}_i$ est le carré d'un idéal ambige $\mathfrak{L}_i$ du corps K qui est alors contenu dans la différente relative.

Car premièrement si $\mathfrak{l}_i$ est contenu dans μ à un degré impair, on a évidemment

$$\mathfrak{l}_i = \left(\mathfrak{l}_i, \frac{\beta}{\gamma}\sqrt{\mu}\right)^2 = \mathfrak{L}_i^2,$$

et $\mathfrak{L}_i$ est un idéal ambige du corps supérieur différent de (1).

Par contre si $\mathfrak{l}_i$ y est à une puissance paire et si

$$\mu \equiv \nu^2, \quad (\mathfrak{l}_i^{2g_i+a_i})$$

n'est possible que pour $g_i < l_i$, on peut déterminer l'entier

$$\mathrm{A} = \frac{\alpha + \beta\sqrt{\mu}}{\gamma},$$

tel que $N_k(\mathrm{A})$ soit divisible par $\mathfrak{l}_i$. Par hypothèse γ est divisible par $\mathfrak{l}_i^{g_i+\bar{a}_i}$ et α l'est par $\mathfrak{l}_i^{\bar{a}_i}$, il ne reste plus qu'à faire voir que l'on peut choisir α et β tels que

$$\alpha^2 - \beta^2\mu \equiv 0 \quad (\mathfrak{l}_i^{2g_i+\bar{a}_i+1}).$$

Posons comme dans la démonstration du premier théorème

$$\mu = \frac{\lambda^2}{\sigma^2}\mu^*, \qquad \alpha = \frac{\lambda}{\sigma}\alpha^*,$$

où λ est exactement divisible par $\mathfrak{l}_i^{a_i}$ et non par une puissance supé-

rieure et où σ est premier avec $\mathfrak{l}_i$, ou α^* et β^* sont premiers avec $\mathfrak{l}_i$, il reste à déterminer α^* et β tels que

(1) $$\alpha^{*2} - \beta^2\mu^* \equiv 0 \ (\mathfrak{l}_i^{2g_i+1}).$$

Comme β est premier avec $\mathfrak{l}_i$ cette congruence équivaut à

(2) $$\xi^2 - \mu^* \equiv 0 \ (\mathfrak{l}_i^{2g_i+1}),$$

où il faut de plus

(3) $$\mu^* \equiv \gamma^{*2}. \ (\mathfrak{l}_i^{2g_i}).$$

Si (2) est un idéal premier du sous-corps k, $g_1 = 0$, et il reste à démontrer que

$$\xi^2 - \mu^* \equiv 0 \ (2)$$

admet toujours une solution.

Mais 2 ne se décompose dans $k(\sqrt{m})$ que si $m \equiv 5 \ (8)$, alors $1, \omega = \frac{1+\sqrt{m}}{2}$ forment une base et on peut poser

$$\xi = x + y\omega, \qquad \mu^* = a + b\omega,$$

comme

$$\omega^2 = \frac{m-1}{4} + \omega \qquad \text{et} \qquad \frac{m-1}{4} \equiv 1 \ (2),$$

on a

$$\xi^2 - \mu = x^2 + y^2 - a + (y^2 - b)\omega \equiv 0 \ (2),$$

cette congruence admet toujours une solution car

$$x^2 + y^2 - a \equiv 0 \ (2)$$

et

$$y^2 - b \equiv 0 \ (2)$$

en admettent toujours.

Deuxièmement si 2 se décompose dans k, $(2) = \mathfrak{l}_1\mathfrak{l}_2$ ou $(2) = \mathfrak{l}_1^2$, il s'agit de savoir dans le premier cas si

(4) $$\xi^2 - \mu^* \equiv 0 \ (\mathfrak{l}_1),$$

et dans le second si

(5) $$\xi^2 - \mu^* \equiv 0 \ (\mathfrak{l}_1)$$

ou

(6) $$\xi^2 - \mu^* \equiv 0 \ (\mathfrak{l}_1^3)$$

est possible.

Chacun de ces trois cas admet une solution. Considérons d'abord le dernier (6)

$$\xi^2 - \mu^* \equiv 0 \ (\mathfrak{l}_1^2)$$

a une solution, car par hypothèse

$$\mu \equiv \nu^2, \ (\mathfrak{l}_1^{2+a_1}),$$

il en résulte

$$\mu^* = \nu^{*2}, \ (\mathfrak{l}_1^2),$$

et $\xi = \nu^*$.

Si $\xi = \nu^*$ n'est pas un nombre du corps tel que

$$\xi^2 - \mu^* \equiv 0 \ (\mathfrak{l}_1^3),$$

on posera

$$\xi_1 = \xi + \lambda\varkappa,$$

où λ est un nombre divisible par $\mathfrak{l}_1$ et non par $\mathfrak{l}_1^2$.

La congruence

$$\xi_1^2 - \mu \equiv 0 \ (\mathfrak{l}_1^3)$$

est alors équivalente à

$$\frac{\xi^2 - \mu^*}{2} + \varkappa^2 \frac{\lambda^2}{2} \equiv 0 \ (\mathfrak{l}_1),$$

mais comme $\frac{\lambda^2}{2}$ est premier avec $\mathfrak{l}_1$ cette congruence est de la même forme que

$$\xi^2 - \mu^* \equiv 0 \ (\mathfrak{l}_1).$$

forme des deux congruences que nous n'avons pas encore étudiées. On a $n(\mathfrak{l}_i) = 2$, tout nombre du corps est donc congru à un nombre entier rationnel impair, et la congruence

$$\xi^2 - \mu \equiv 0 \ (\mathfrak{l}_i)$$

admet une solution, car

$$x^2 - a \equiv 0 \pmod 2$$

est toujours possible en nombres entiers.

Dans tous les cas considérés l_i se décompose donc dans le corps relatif.

$$\left(l_i, \frac{\alpha + \beta\sqrt{\mu}}{\gamma}\right) = \left(l_i, \frac{\alpha + \beta\sqrt{\mu}}{\gamma}, 2\right)$$

est un idéal qui contient aussi $\frac{\alpha - \beta\sqrt{\mu}}{\gamma}$, car

$$\left(\frac{\alpha + \beta\sqrt{\mu}}{\gamma}\right) + \left(\frac{\alpha - \beta\sqrt{\mu}}{\gamma}\right) \equiv 0 \ (l_i),$$
$$\left(\frac{\alpha + \beta\sqrt{\mu}}{\gamma}\right) - \left(\frac{\alpha - \beta\sqrt{\mu}}{\gamma}\right) \equiv 0 \ (l_i),$$

et tous les idéaux considérés sont ambiges.

Nous avons donc démontré la première partie du théorème.

Reste à faire voire que $\mathfrak{D}_k$ contient tous les idéaux ambiges. Soit $\mathfrak{P}$ un idéal ambige

$$\mathfrak{p} = \mathfrak{P}^2,$$
$$n(\mathfrak{p}) = n(\mathfrak{P}^2) = N(\mathfrak{P}).$$

Il en résulte que l'on peut former un système complet de restes suivant $\mathfrak{P}$, composé uniquement de nombres du sous-corps k, car tout nombre qui n'est pas divisible par $\mathfrak{p}$ ne peut l'être par $\mathfrak{P}$. Par conséquent tout nombre du corps relatif est congru à un nombre du corps de base suivant un idéal ambige $\mathfrak{P}$,

$$A \equiv \alpha, \ (\mathfrak{P}).$$

donc aussi

$$S(A) \equiv \alpha, \ (\mathfrak{P}),$$

et par suite

$$A - S(A) \equiv 0, \ (\mathfrak{P}).$$

Mais tous les nombres de $\mathfrak{D}_k$ sont contenus dans $\mathfrak{P}$ et par suite $\mathfrak{D}_k$ est divisible par $\mathfrak{P}$.

Le théorème 3 est complètement démontré.

Remarque. — [Il résulte du théorème 3 qu'un idéal $\mathfrak{l}_i$ qui ne divise pas le discriminant relatif, ou bien ne peut se décomposer dans le corps relatif, ou bien il se décompose en un produit de deux idéaux premiers non ambiges.

En effet on a alors $\mu \equiv \nu^2$, $(\mathfrak{l}_i^{l_i+a_i})$ et le dénominateur γ de l'entier $\frac{\alpha + \beta\sqrt{\mu}}{\gamma}$ contient $\mathfrak{l}_i^{l_i+a_i}$, tandis que β est premier avec $\mathfrak{l}_i$. Dans le cas où $\mathfrak{L}_i = \left(\mathfrak{l}_i, \frac{\alpha + \beta\sqrt{\mu}}{\gamma}\right)$ est un facteur premier de $\mathfrak{l}_i$, on a nécessairement

$$\left(\mathfrak{l}_i, \frac{\alpha + \beta\sqrt{\mu}}{\gamma}, \frac{\alpha - \beta\sqrt{\mu}}{\gamma}\right) = (1),$$

car $\left(\frac{2\beta\sqrt{\mu}}{\gamma}\right)^2$ est premier avec $\mathfrak{l}_i$].

4e *Théorème.* — Tout idéal premier du corps de base k qui divise le discriminant relatif, est égal dans le corps relatif au carré d'un idéal premier ambige. Réciproquement, tout idéal premier $\mathfrak{p}$ du corps de base divisible par le carré d'un idéal premier du corps relatif, est contenu dans le discriminant relatif $\mathfrak{d}$.

Démonstration : Soit $\mathfrak{P}$ un idéal ambige du corps relatif, dont le carré est un idéal premier $\mathfrak{p}$ de k, $\mathfrak{P}$ est un facteur de la différente relative et par suite $\mathfrak{P}^2 = \mathfrak{p}$ divise le discriminant relatif, car $\mathfrak{d} = \mathfrak{D}_k^2$.

Donc tout idéal de k qui est le carré d'un idéal ambige divise le discriminant relatif. Soit de plus $\mathfrak{p} = \mathfrak{P}^2\mathfrak{Q}$, on a aussi

$$\mathfrak{p} = S(\mathfrak{P})^2 S(\mathfrak{Q}),$$

d'où il résulte que

$$\mathfrak{P} = S(\mathfrak{P}), \qquad \mathfrak{Q} = S(\mathfrak{Q}),$$

et comme $\mathfrak{P}S(\mathfrak{P})$ est un idéal de k il faut que $\mathfrak{Q} = 1$, $\mathfrak{p}$ est le carré d'un idéal ambige.

Enfin si $\mathfrak{p}$ divise $\mathfrak{d}$, il divise $\mathfrak{D}_k^2$, il faut donc que $\mathfrak{p} = \mathfrak{P}^2$, car $\mathfrak{D}_k$ ne contient comme facteurs que les idéaux ambiges de $K(\sqrt{\mu})$ et qu'il les contient tous.

Les théorèmes que nous venons de démontrer sont des théorèmes généraux. Nous allons exposer maintenant sur divers exemples

numériques l'idée fondamentale de nouvelles recherches. (Voir le travail de M. Hilbert que nous avons cité). Les théorèmes du numéro suivant, doivent nous conduire à notre but : L'exposé et la démonstration des lois les plus simples de réciprocité dans le corps de base $k(\sqrt{m})$.

53. Le discriminant relatif d'un sur-corps par rapport à un corps de base imaginaire dont le nombre des classes est impair. — Nous allons prendre tout d'abord un corps k pour lequel nous supposerons (Hilbert, *Math. Ann.*, 51, p. 27) :

1° qu'il est imaginaire ;

2° le nombre de ses classes est impair.

Tout corps relatif $K(\sqrt{\mu})$ est également imaginaire. Pris d'une façon absolue $K(\sqrt{\mu})$ est un corps imaginaire du quatrième degré ainsi que tous ses conjugués.

A l'aide du théorème de Minkowski comme au n° 47 on démontrera qu'il existe dans le corps une seule unité fondamentale différente de ± 1, E dont la norme est une unité dans le corps de base k, c'est-à-dire $= \pm 1$, si nous excluons les corps $k(\sqrt{-1})$ et $k(\sqrt{-3})$.

La deuxième condition nous apprend de plus : Les théorèmes qui donnent le nombre des genres d'un corps quadratique k disent que le nombre est toujours pair lorsque le discriminant du corps contient plus d'un facteur premier et alors le nombre des classes est pair.

La deuxième condition n'est donc remplie que si m est un nombre premier négatif de la forme $m \equiv 1 \ (4)$ ou si $m = -1$, $m = -2$.

M. Dörrie a étudié complètement le corps $k(\sqrt{-3})$, les lois de réciprocité dans ce corps et ses sous-corps. Nous renverrons à ses travaux et nous n'étudierons pas ici le cas $k(\sqrt{-3})$ pas plus que le corps $k(\sqrt{-1})$ qui a été traité déjà par Gauss. Nous aurons donc à considérer les corps $k(\sqrt{-2})$, $\sqrt{-7}$, $\sqrt{-11}$, $\sqrt{-19}$, $\sqrt{-23}$, $\sqrt{-31}$, $\sqrt{-43}$, $\sqrt{-47}$, etc., dont les nombres de classes respectifs sont

$$1, \quad 1, \quad 1, \quad 1, \quad 3, \quad 3, \quad 1, \quad 5.$$

Théorème. — Lorsque $k(\sqrt{m})$ est un corps imaginaire pour lequel h est impair, le discriminant relatif de tout corps relatif par rapport au corps $k(\sqrt{m})$ est différent de ± 1.

Démonstration : D'après les théorèmes sur le discriminant relatif du corps $K(\sqrt{m})$, celui-ci contient en facteur :

1° un idéal $\mathfrak{p}$ de k premier avec 2, si μ est divisible par une puissance impaire de $\mathfrak{p}$;

2° l'idéal $\mathfrak{l}$ de k que divise (2) dans le cas où μ est divisible par $\mathfrak{l}^a$, que (2) est divisible par $\mathfrak{l}^l$ et que

$$\mu \equiv \alpha^2, \ (\mathfrak{l}^{2l-a})$$

n'est satisfaite par aucun nombre α du corps k.

Il a déjà été démontré que cette dernière congruence n'est possible que si $a = 2e$. Admettons donc que μ est divisible par

$$\mathfrak{p}_1 \cdot \mathfrak{p}_2, \ldots \mathfrak{l}.$$

le discriminant relatif ne poura être premier avec tous ces nombres que si

$$(\mu) = \mathfrak{p}_1^{2e_1} \mathfrak{p}_2^{2e_2} \ldots \mathfrak{l}^{e2},$$

on aurait donc

$$\mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_2} \ldots \mathfrak{l}^{e})^2 \sim 1,$$

mais d'autre part

$$(\mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_2} \ldots \mathfrak{l}^{e})^h \sim 1.$$

et h est impair, on aurait aussi

$$\mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_2} \ldots \mathfrak{l}^{e} \sim 1.$$

On aurait donc $\mu = \varepsilon\nu^2$, où ε est une unité et ν un nombre entier.

Mais le corps $K(\sqrt{\varepsilon\nu^2})$ coïnciderait alors avec $K(\sqrt{\varepsilon})$.

Pour démontrer que le discriminant relatif est différent de ± 1, il suffit d'après le dernier théorème du n° 51 de démontrer que dans $k(\sqrt{m})$

$$\varepsilon \equiv \alpha^2, \ (4)$$

n'est pas possible.

Comme on a écarté $k(\sqrt{-1})$ et $k(\sqrt{-3})$ on ne peut avoir que $\varepsilon = -1$, il s'agit de savoir si

$$-1 \equiv (x + y\omega)^2, \ (4)$$

est possible en entiers rationnels x et y.

Soit

$$\omega = \frac{1 + \sqrt{m}}{2}, \qquad \omega^2 = \frac{m-1}{4} + \omega,$$

ce qui donne

$$-1 \equiv x^2 + \frac{m-1}{4} y^2 + (2xy + y^2)\omega, \ (4),$$

c'est-à-dire

$$x^2 + \frac{m-1}{4} y^2 + 1 \equiv 0, \ (4),$$
$$2xy + y^2 \equiv 0, \ (4).$$

La dernière exige que y soit pair, il ne nous reste alors que

$$x^2 + 1 \equiv 0, \ (4),$$

mais cette dernière est impossible, c'est-à-dire qu'on ne peut avoir

$$\varepsilon \equiv \alpha^2, \ (4).$$

Le discriminant relatif de $K(\sqrt{\varepsilon})$ n'est pas premier avec 2, il est donc différent de ± 1.

54. Quelques cas simples de la loi de réciprocité quadratique de M. Hilbert. — *Théorème.* — Un nombre entier ou fractionnaire B du corps relatif $K(\sqrt{\mu})$, dont la norme relative par rapport à k est $+1$, peut être représenté par le quotient de deux entiers conjugués du corps relatif, c'est-à-dire $B = \frac{A}{S(A)}$.

Démonstration : Soit (voir n° 23) $B \neq -1$,

$$A_1 = 1 + B,$$
$$S(A_1) = 1 + S(B) = \frac{1}{B}(1 + B),$$

et par suite $B = \frac{A_1}{S(A_1)}$.

Si donc on choisit un nombre rationnel entier a, tel que aA_1 soit entier, $aS(A_1)$ est aussi entier. $A = aA_1$ répond à la question, car $B = \frac{A}{S(A)}$.

On pourrait encore démontrer ce théorème par des considérations valables pour tout corps de base.

Par hypothèse $BS(B) = 1$, soit θ un nombre qui détermine le corps relatif et posons

$$B_x = \frac{x + \theta}{x + S(\theta)} B$$

et

$$A_x = 1 + B_x.$$

Il en résulte d'abord

$$B_x = \frac{A_x}{S(A_x)},$$

car les dernières égalités nous donnent

$$B_x S(A_x) = B_x(1 + S(B_x)) = B_x + 1 = A_x.$$

Prenons pour x un nombre rationnel a tel que B_a ne soit pas nul, ce qui est toujours possible, on peut poser

$$A_1 = \frac{A_a}{a + \theta},$$

d'où

$$B = \frac{A_1}{S(A_1)} = \frac{a + S(\theta)}{a + \theta} \frac{A_a}{S(A_a)} = \frac{a + S(\theta)}{a + \theta} B_a.$$

Soit $A_1 = \frac{A}{b}$ où A est un entier du corps relatif et b un nombre rationnel, il vient

$$B = \frac{A}{S(A)},$$

ce que nous voulions démontrer.

Théorème. — Lorsque le discriminant relatif de $K(\sqrt{\mu})$ ne contient qu'un seul idéal premier $\mathfrak{p}$ de k, la norme relative de l'unité fondamentale E de K égale -1.

Démonstration : Soit E l'unité fondamentale du corps $K(\sqrt{\mu})$. Admettons que $N_r(E) = +1$, il y a dans K un nombre A tel que

$$E = \frac{A}{S(A)} \quad \text{ou} \quad A = ES(A).$$

Tout nombre qui divise A divise par conséquent S(A). Ceci exige que A ne soit divisible que par des idéaux ambiges de K et en outre peut-être par certains idéaux du corps de base.

D'après l'hypothèse le surcorps $K(\sqrt{\mu})$ ne contient qu'un seul idéal ambige $\mathfrak{P}$. Mais il y a toujours dans le corps fondamental un idéal $\mathfrak{m}$ tel que $\mathfrak{m} \cdot \mathfrak{P} = \frac{\xi\sqrt{\mu}}{\gamma}$ où ξ et γ ont le même sens que dans le théorème relatif à la base du corps, de plus comme le corps de base imaginaire n'a d'autre unité que ± 1, c'est-à-dire $N_k(E) = \pm 1$, on peut toujours admettre que A est de la forme

$$A = H\alpha \qquad \text{ou} \qquad A = H \cdot \xi\sqrt{\mu},$$

où α est un entier, ξ un nombre entier ou fractionnaire de $k(\sqrt{m})$ et où H est une unité du corps relatif.

D'où

$$E = \frac{A}{S(A)} = \frac{H}{S(H)} = \pm H^2.$$

E ne serait pas une unité fondamentale.

Il faut donc que $N_k(E) = -1$.

Remarque. — (Rappelons que $k(\sqrt{-1})$ et $k(\sqrt{-3})$ sont exceptés dans ces recherches. On verrait dans chaque cas comment ce théorème doit être modifié).

On peut conclure de là maintenant que le nombre des classes H de ce corps $K(\sqrt{\mu})$ est impair. (Comparer avec le nº 23).

Admettons que le nombre des classes soit pair. Il y a un idéal non principal $\mathfrak{J}$ tel que $\mathfrak{J}^2 \sim 1$. Mais alors $S(\mathfrak{J})^2 \sim 1$ et $(\mathfrak{C})S(\mathfrak{J})^2 \sim 1$.

Mais comme $\mathfrak{J}S(\mathfrak{J}) = \mathfrak{j}$ est un idéal du corps de base et que $\mathfrak{j}^h \sim 1$, l'hypothèse de h impair exige que $\mathfrak{J}S(\mathfrak{J}) \sim 1$. Mais comme $\mathfrak{J}^2 \sim 1$, $\mathfrak{J}S(\mathfrak{J}) \sim 1$ on en conclut que $\mathfrak{J} \sim S(\mathfrak{J})$ ou $\mathfrak{J} = (B)S(\mathfrak{J})$ où B est un entier ou un nombre fractionnaire de K dont la norme relative $N_k(B) = \pm 1$, le corps k n'ayant pas d'autres unités que ± 1. Si $N_k(B) = +1$ on peut poser $B = \frac{S(A)}{A}$ où A et S(A) sont des entiers du corps, mais si $N_k(A) = -1$, $N_k(EB) = +1$ et l'on peut poser $EB = \frac{S(A)}{A}$. Dans les deux cas

$$\mathfrak{J} = (B)S(\mathfrak{J}) \qquad \text{peut s'écrire} \qquad A\mathfrak{J} = S(A\mathfrak{J}).$$

c'est-à-dire que tout facteur idéal premier $(A)\mathfrak{J}$ serait aussi facteur de $S(A\mathfrak{J})$.

Mais comme $k(\sqrt{\mu})$ ne contient qu'un seul idéal ambige et que l'on peut toujours trouver un nombre $\mathfrak{m}$ du corps k tel que

$$\mathfrak{m} . \mathfrak{P} = \left(\frac{\beta\sqrt{\mu}}{\gamma}\right),$$

on a ou bien

$$(A)\mathfrak{J} = \mathfrak{j} \quad \text{ou bien} \quad (A)\mathfrak{J} = \mathfrak{j}\left(\frac{\beta\sqrt{\mu}}{\gamma}\right),$$

où $\mathfrak{j}$ est un idéal de k. Dans les deux cas $\mathfrak{J}$ serait équivalent à un idéal du corps de base, c'est-à-dire à un idéal principal, et comme alors on aurait $\mathfrak{J}^h \sim \mathfrak{j}^h \sim 1$ en même temps que $\mathfrak{J}^2 \sim 1$ on aurait $\mathfrak{J} \sim 1$, ce qui est contraire à l'hypothèse.

M. Hilbert pour formuler plus facilement les théorèmes suivants a introduit dans son étude du corps relatif quadratique et du corps relatif abélien les désignations suivantes [1].

Définition : Un idéal premier $\mathfrak{p}$ du corps de base $k(\sqrt{m})$ premier avec (2), et suivant lequel toute unité du corps $k(\sqrt{m})$ est reste quadratique est dit un idéal *primaire*, tout idéal qui ne satisfait pas à cette condition est un idéal non primaire.

Comme d'ailleurs par hypothèse les unités du corps de base sont ± 1, tout idéal premier avec 2 est primaire s'il est reste quadratique de -1.

On a alors le théorème suivant :

Théorème. — Soit $\mathfrak{p}$ un idéal primaire de k, il y a toujours un nombre π du corps, tel que $(\pi) = \mathfrak{p}^h$ et tel que

$$\pi \equiv \alpha^2, (4)$$

soit satisfaite par un α entier du corps.

Démonstration : Les hypothèses restreintes que nous avons faites facilitent la démonstration.

$\mathfrak{p}$ est un idéal soit du premier soit du second degré. Dans le dernier cas $\mathfrak{p} = (p)$, et comme $\mathfrak{p}$ et p sont premiers avec 2, on a certainement

$$p \equiv 1 \ (4) \quad \text{ou} \quad -p \equiv 1 \ (4).$$

Dans ce cas le théorème est donc démontré.

---

[1] La notion et le mot d'idéal primaire sont dûs à Gauss. *Œuvres*, t. II, *Théorie résidus biquadratiques*, *Com. soc.* Wr. 36.

Par contre soit $\mathfrak{p}$ un idéal du premier degré

$$(p) = \mathfrak{p} \cdot \mathfrak{p},$$

$n(\mathfrak{p}) = p$, et p est impair.

On a toujours

$$\xi^{n(\mathfrak{p})-1} \equiv 1, \ (\mathfrak{p}).$$

Pour que $-1 \equiv \xi^2, (\mathfrak{p})$ soit possible pour un entier du corps $k(\sqrt{m})$ il faut que

$$\frac{n(\mathfrak{p})-1}{2} \equiv 0, (2) \quad \text{c'est-à-dire} \quad p \equiv 1, (4).$$

Soit

$$\mathfrak{p}^h = (a + b\omega),$$

où

$$\omega = \frac{1+\sqrt{m}}{2}.$$

alors

$$(p^h) = (a + b\omega)(a + b\omega')$$
$$= \left(a^2 + ab + b^2 \frac{1+m}{4}\right),$$

comme $p \equiv 1, (4)$, a et b ne peuvent être tous deux pairs, et comme

$$a^2 + ab + b^2 \frac{1-m}{4} = \left(a + \frac{b}{2}\right)^2 - \frac{m}{4} b^2$$

est toujours positif on a pour a et b les cas suivants :

1° Si $\frac{1-m}{4} \equiv 1, (4)$, $a \equiv \pm 1$, $b \equiv 0$ ou $a \equiv \pm 1$, $b \equiv \mp 1, (4)$.

2° Si $\frac{1-m}{4} \equiv 2, (4)$, $a \equiv \pm 1$, $b \equiv 0, (4)$.

3° Si $\frac{1-m}{4} \equiv 3, (4)$, $a \equiv \pm 1$, $b \equiv 0$ ou $a \equiv \pm 1$ avec $b \equiv \pm 1$ ou $a \equiv 2$, $b \equiv \pm 1, (4)$.

4° Si $\frac{1-m}{4} \equiv 0, (4)$, $a \equiv \pm 1$, $b \equiv 0, (4)$.

En tenant compte de tous ces cas on voit qu'en effet l'une des congruences

$$a - b\omega \equiv (x + y\omega)^2, (4$$
$$- a - b\omega \equiv (x + y\omega)^2, (4$$

est toujours satisfaite par des entiers rationnels x et y. Autrement dit le système

$$a - x^2 + \frac{1-m}{4} y^2 \equiv 0, (4)$$

$$b + 2xy - y^2 \equiv 0, (4)$$

ou bien

$$-a - x^2 + \frac{1-m}{4} y^2 \equiv 0, (4)$$

$$-b - 2xy - y^2 \equiv 0, (4)$$

admet des solutions entières x et y.

Le théorème est démontré, on a toujours

$$\pi = \pm (a + b\omega) = \alpha^2, (4).$$

Théorème réciproque. — Soit π un entier du corps k, pour lequel $\pi \equiv \alpha^2, (4)$ admet une solution entière, et si (π) est la h' puissance d'un idéal premier $\mathfrak{p}$ premier avec (2), c'est-à-dire $(\pi) = \mathfrak{p}^h$, $\mathfrak{p}$ est un idéal primaire, c'est-à-dire que -1 est reste quadratique de $\mathfrak{p}$.

Démonstration : Par suite de l'hypothèse le discriminant du corps relatif $K(\sqrt{\pi})$ ne contient qu'un facteur premier $\mathfrak{p}$. Mais alors la norme relative de l'unité fondamentale $\mathbf{E}$ du corps $K(\sqrt{\pi})$ est égale à -1. Posons $\mathbf{E} = \frac{\sigma + \rho\sqrt{\pi}}{2\tau}$ (c'est la forme des nombres entiers du corps $K(\sqrt{\pi})$) $\frac{2\sigma}{2\tau}$ est un nombre entier et τ est au plus divisible par $\mathfrak{p}^{\frac{h-1}{2}}$. De l'égalité

$$-1 = \frac{\sigma^2 - \rho^2\pi}{4\tau^2},$$

il résulte donc

$$-4 \equiv \lambda^2, \left(\frac{\rho^2\pi}{\tau^2}\right),$$

et *a fortiori*

$$-4 \equiv \lambda^2, (\mathfrak{p}).$$

Comme 2 est premier avec $\mathfrak{p}$ il y a un nombre ξ tel que

$$2\xi = \pm 1 \ (\mathfrak{p}) \qquad \text{ou} \qquad 4\xi^2 \equiv 1 \ (\mathfrak{p}),$$

on obtient finalement

$$-1 \equiv \alpha^3 \ (\mathfrak{p}),$$

ce qu'il fallait démontrer.

Ces théorèmes justifient la définition suivante :

Définition. — Soit $\mathfrak{p}$ un idéal primaire du corps k et si $(\pi) = \mathfrak{p}^h$ est choisi de façon que $\pi \equiv \alpha^2, (4)$, π est dit un *nombre primaire* de l'idéal primaire $\mathfrak{p}$.

Théorème. — Soit $\mathfrak{p}$ un idéal primaire du corps k et π un nombre primaire de $\mathfrak{p}$, soit de plus $\mathfrak{r}$ un autre idéal premier de k, soit $(\rho) = \mathfrak{r}$, $\left(\frac{\pi}{\mathfrak{r}}\right) = +1$ entraîne $\left(\frac{\rho}{\mathfrak{p}}\right) = +1$.

$\left(\frac{\pi}{\mathfrak{r}}\right)$ représente le symbole de Legendre étendu aux idéaux.

Démonstration : L'hypothèse $\left(\frac{\pi}{\mathfrak{r}}\right) = +1$ exige que l'idéal premier $\mathfrak{r}$ se décompose dans le corps relatif $K(\sqrt{\pi})$ en un produit de deux idéaux conjugués relatifs

$$\mathfrak{r} = (\mathfrak{r}, A)(\mathfrak{r}, S(A)).$$

Comme de plus π est un nombre primaire de $\mathfrak{p}$, le discriminant relatif de $K(\sqrt{\pi})$ ne contient que le facteur premier $\mathfrak{p}$, et il existe un nombre rationnel entier impair tel que

$$\mathfrak{r}^u = (P)(S(P)),$$

où P, $S(P)$ sont des entiers du corps relatif $K(\sqrt{\pi})$. Si on élève les deux membres à la puissance h

$$(\rho)^u = (P_1)(S(P_1)),$$

$$\rho^u = \frac{\alpha + \beta\sqrt{\pi}}{2\gamma} \cdot \frac{\alpha - \beta\sqrt{\pi}}{2\gamma},$$

$\frac{\alpha}{\gamma}$, $\frac{\beta\sqrt{\pi}}{\gamma}$ sont des entiers du corps relatif et on a

$$4\rho^u \equiv \nu^2, (\mathfrak{p})$$

Déterminons ξ tel que

$$2\rho^{\frac{u-1}{2}}\xi \equiv 1, (\mathfrak{p}),$$

on a

$$4\xi^2\rho^u \equiv \rho \equiv \xi^2\nu^2, (\mathfrak{p}),$$

et enfin

$$\rho \equiv \alpha^2, (\mathfrak{p}),$$

c'est-à-dire

$$\left(\frac{2}{\mathfrak{p}}\right) = +1.$$

En appliquant plusieurs fois ce théorème on voit que

Théorème. — Soit $\mathfrak{p}$ et $\mathfrak{p}_1$ deux idéaux premiers primaires et π, π_1 deux nombres primaires appartenant l'un au premier l'autre au second, on voit que

$$\left(\frac{\pi}{\mathfrak{p}_1}\right) = \left(\frac{\pi_1}{\mathfrak{p}}\right).$$

Démonstration : De $\left(\frac{\pi}{\mathfrak{p}_1}\right) = -1$ il résulte que $\left(\frac{\pi_1}{\mathfrak{p}}\right) = +1$, mais si $\left(\frac{\pi}{\mathfrak{p}_1}\right) = -1$, $\left(\frac{\pi_1}{\mathfrak{p}}\right) = -1$, car si on avait $\left(\frac{\pi_1}{\mathfrak{p}}\right) = +1$ on aurait $\left(\frac{\pi}{\mathfrak{p}_1}\right) = +1$ ce qui est contraire à l'hypothèse.

Nous avons là une faible quoique importante partie (les théorèmes complémentaires) du théorème général de réciprocité. Pour ce qui concerne le théorème général nous renverrons le lecteur aux travaux de MM. Hilbert et Furtwängler. Le symbole de M. Hilbert concernant les restes normiques et les non-restes normiques permet de formuler simplement cette loi généralisée par rapport à un corps de base quelconque. A l'aide de ce symbole les classes d'idéaux du corps relativement quadratique peuvent être réparties en genres. En démontrant l'existence de certains genres parmi tous les possibles on atteint la loi de réciprocité (1).

Dans les cas que nous venons de considérer, nous avons pu arriver à une démonstration grâce à ce fait que le nombre des classes du corps relatif étant impair toutes ces classes appartiennent au même genre.

55 Exemples de corps de classe. — Pour terminer nous indiquerons encore les propriétés du corps relatif dans quelques cas exclus jusqu'ici :

---

(1) Voir D. Hilbert, *Math. Ann.*, t. LI. *Das allgemeine quadratische Reziprozitätsgesetz.* M. Dorrie a démontré cette loi pour les corps dont le nombre des classes est 1, dans sa dissertation déjà citée. On trouve des exemples numériques dans la thèse de G. Rückle, Göttingen, 1901.

1° Quand le corps de base est imaginaire et que le nombre des classes est pair ;

2° Quand le corps de base est réel.

1er *Exemple.* — Soit $k(\sqrt{-5})$ le corps de base dont les seules unités sont ± 1. Les nombres 1, $\omega = \sqrt{-5}$ forment une base du corps dont le nombre des classes est $h = 2$.

La première question qui nous intéresse est la suivante : Y a-t-il un corps relatif quadratique dont le discriminant relatif par rapport à k est ± 1. Un pareil corps relatif ne contient évidemment pas d'idéal ambige et nous l'appellerons un *surcorps non ramifié* (unverzweigter Oberkörper).

Comme le nombre $\mu = -1$ du corps $k(\sqrt{-5})$ ne contient aucun facteur premier et que

$$-1 = \alpha^2, \quad (4)$$

est satisfaite pour $\alpha = \sqrt{-5}$, le discriminant relatif de $K(\sqrt{-1})$ est premier avec (2) et ne contient aucun facteur premier, c'est-à-dire que $K(\sqrt{-1})$ est un corps répondant à la définition.

M. Hilbert dit qu'un corps quadratique relatif $K(\sqrt{\mu})$ dont le discriminant relatif par rapport à un sous-corps ayant un nombre de classes $h = 2$ est égal à ± 1 est un corps de classe de ce sous-corps [1].

Dans l'exemple choisi $K(\sqrt{-1})$ est un corps de classe du corps quadratique de base $k(\sqrt{-5})$.

Si l'on prend comme base de ce corps de classe

$$1, \quad \omega = \sqrt{-5}, \quad \Omega = \frac{\sqrt{-5} + \sqrt{-1}}{2}, \quad \Omega_1 = \sqrt{-5}\,\frac{\sqrt{-5} + \sqrt{-1}}{2}.$$

---

[1] Les notions et les théorèmes exposés dans ce numéro à l'aide de quelques exemples se rattachent à des notions correspondantes de la théorie de la multiplication complexe des fonctions elliptiques. Kronecker en a été l'initiateur, l'expression corps de classe lui est due. Voir D. Hilbert, *Nachr. von der kgl. Ges. d. Wissensch. zu Göttingen, math.-phys. Klasse*, 1898, p. 370 et suiv. *Acta math.*, t. XXVI, 1902, p. 99 et suiv. Ce mémoire est un complément de celui des *Math. Ann.*, t. LI, sur les corps quadrat. relat. Voir aussi R. Fueter, *Dissertation. Der Klassenkörper der quadratischen Körper und die komplexe Multiplication*, Göttingen, 1903, chap. I, II.

Ω est à la fois une unité telle que

$$\Omega S(\Omega) = \frac{-5+1}{4} = -1.$$

Lorsqu'on étudie la décomposition des nombres et des idéaux du corps de base on obtient les résultats suivants. Chaque proposition exprime une propriété générale caractéristique du corps de classe.

1. Un nombre premier p indécomposable dans $k(\sqrt{-5})$ se décompose en un produit de deux idéaux premiers dans le corps relatif $K(\sqrt{-1})$, car si $\left(\frac{-20}{p}\right) = \left(\frac{-5}{p}\right) = -1$ on a $\left(\frac{5}{p}\right) = +1$ ou encore $\left(\frac{-1}{p}\right) = +1$. Il en résulte que p se décompose dans $k(\sqrt{+5})$ ou $k(\sqrt{-1})$ et comme tous les nombres de ces deux corps appartiennent au corps relatif $K(\sqrt{-1})$ p se décompose dans ce dernier.

Par exemple $(p) = 11$ est un idéal premier de second degré dans $k(\sqrt{-5})$ on a $\left(\frac{5}{11}\right) = 1$

$$(11) = (4+\sqrt{5})(4-\sqrt{5}) = (9+2\Omega_1)(1-2\Omega_1).$$

De même $p = 13, 17, 19, 31$ sont indécomposables dans $k(\sqrt{-5})$, par contre dans le corps relatif

$$(13) = (3-2\sqrt{-1})(3-2\sqrt{-1}) = (3-2\omega-4\Omega)(3+2\omega-4\Omega).$$

$$(17) = (4+\sqrt{-1})(4-\sqrt{-1}) = (4-\omega+2\Omega)(4+\omega-2\Omega).$$

$$(19) = \left(4+\frac{1+\sqrt{5}}{2}\right)\left(4+\frac{1-\sqrt{5}}{2}\right) = (7+\Omega_1)(2-\Omega_1).$$

$$(31) = (6+\sqrt{5})(6-\sqrt{5}) = (11+2\Omega_1)(1-2\Omega_1).$$

2. Si p est un nombre premier qui se décompose dans $k(\sqrt{-5})$ en un produit $\mathfrak{p}.\mathfrak{p}'$ il faut distinguer deux cas, ou bien $p \equiv 1\ (4)$ ou bien $p \equiv 3\ (4)$.

2*a*. Dans le premier cas

$$-1 \equiv \alpha^2\ (\mathfrak{p})$$

est toujours possible en nombre entier du corps de base. En effet

comme $n(\mathfrak{p}) = p$ tout nombre entier de k est congru à un entier rationnel compris entre 1 et p suivant le module $(\mathfrak{p})$, et comme

$$-1 \equiv x^2 \ (p)$$

admet une solution, *a fortiori*

$$-1 \equiv \alpha^2 \ (\mathfrak{p})$$

est possible ainsi que

$$-1 \equiv \alpha^2 \ (\mathfrak{p}').$$

Les idéaux $\mathfrak{p}$ et $\mathfrak{p}'$ sont donc décomposables à leur tour dans le corps relatif $K(\sqrt{-1})$. Les deux idéaux $\mathfrak{p}$ et $\mathfrak{p}'$ sont des idéaux principaux, comme nous allons le faire voir. Le corps de base $k(\sqrt{-5})$ a pour discriminant -20 qui contient deux facteurs premiers 2 et 5. Les deux classes (la classe principale et la non principale) appartiennent donc à deux genres différents, et l'on voit de suite que $\mathfrak{p}$, $\mathfrak{p}'$ appartiennent au genre principal et par suite à la classe des idéaux principanx, et en effet comme $p \equiv 1 \ (4)$, $\left(\frac{-1}{p}\right) = 1$, $\left(\frac{\pm 5}{p}\right) = 1$.

2*b*. Le second cas est tout autre. La congruence

$$-1 \equiv \alpha^2 \ (\mathfrak{p})$$

ne peut avoir aucune solution, sans quoi comme α est congru à un nombre rationnel suivant le mod $\mathfrak{p}$

$$-1 \equiv x^2, \ (p)$$

serait possible.

Les idéaux premiers de la seconde classe, c'est-à-dire de la classe des idéaux non principaux sont encore des idéaux premiers dans le corps relatif $K(\sqrt{-1})$. Mais ces idéaux premiers sont des idéaux principaux du surcorps $K(\sqrt{-1})$

En effet 2 se décompose dans $k\sqrt{-1}$,

$$2 = (1 + \sqrt{-1})(1 - \sqrt{-1}).$$

Posons $\mathfrak{z} = (2, 1 + \sqrt{-5})$ et soit $\mathfrak{p}$ un idéal de la seconde classe du corps $k(\sqrt{-5})$ on voit que $\mathfrak{z}\mathfrak{p} = (\alpha)$ où α est un nombre entier du corps de base.

Par suite $\mathfrak{z}^2\mathfrak{p}^2 = (\alpha)^2$ en écrivant $\mathfrak{z}\mathfrak{p} = (\pi)$, on voit que

$$\pm 2\pi = \alpha^2 \quad \text{ou} \quad \pm 4\pi = \alpha^2 . 2.$$

Dans le corps relatif

$$(\pi) = \left(\frac{\alpha(1+\sqrt{-1})}{2}\right)\left(\frac{\alpha(1-\sqrt{-1})}{2}\right),$$

comme

$$\frac{\alpha(1+\sqrt{-1})}{2} \quad \text{et} \quad \frac{\alpha(1-\sqrt{-1})}{2}$$

sont des entiers de $K(\sqrt{-1})$ (leur somme et leur produit sont des entiers), $\mathfrak{p}^2$ est le produit de deux idéaux conjugués relatifs dans le corps $K(\sqrt{-1})$. Comme d'autre part $\mathfrak{p}$ ne se décompose pas dans ce corps et que

$$\frac{\alpha(1-\sqrt{-1})}{2} \quad \text{et} \quad \frac{\alpha(1-\sqrt{-1})}{2}$$

ne se distinguent que par un facteur unité $\sqrt{-1}$ on a dans le corps relatif

$$\mathfrak{p} = \left(\frac{\alpha(1+\sqrt{-1})}{2}\right),$$

c'est-à-dire que tout idéal premier du corps $k(\sqrt{-5})$ qui est un idéal non principal de ce corps devient un idéal principal dans le corps relatif.

Les résultats 1 et 2 nous donnent le

Théorème. — Les idéaux premiers principaux du corps $k(\sqrt{-5})$ se décomposent dans le corps de classe en un produit de deux idéaux, par contre les idéaux premiers non principaux sont encore des idéaux premiers du corps de classe, mais ils y sont des idéaux principaux.

Quelques exemples numériques illustreront ce théorème :

$$(5) = (\sqrt{-5})^2,$$

$$(29) = (3 + 2\sqrt{-5})(3 - 2\sqrt{-5}),$$

$$(41) = (4 + \sqrt{-5})(6 - \sqrt{-5}),$$

$$(61) = (3 + 3\sqrt{-5})(4 - 3\sqrt{-5}),$$

par conséquent $(\sqrt{-5})$, $(3+2\sqrt{-5})$, $(3-2\sqrt{-5})$, etc., sont des idéaux principaux du corps $k(\sqrt{-5})$ qui se décomposent dans le corps de classe. On trouve facilement :

$$(\sqrt{-5}) = (1+\Omega)(1+S(\Omega)),$$

$$(3+2\sqrt{-5}) = (1-\sqrt{-5}+\sqrt{-1})(1-\sqrt{-5}-\sqrt{-1}),$$

$$(3-2\sqrt{-5}) = (1+\sqrt{-5}+\sqrt{-1})(1+\sqrt{-5}-\sqrt{-1}),$$

$$(6+\sqrt{-5})$$

$$= \left(\frac{5+\sqrt{-5}-(3-\sqrt{-5})\sqrt{-1}}{2}\right)\left(\frac{5+\sqrt{-5}+(3-\sqrt{-5})\sqrt{-1}}{2}\right)$$

$$= (5+2\sqrt{-5}-3\Omega+\Omega_1)(5+2\sqrt{-5}-S(\Omega)-S(\Omega_1)),$$

on obtient $6-\sqrt{-5}$ en remplaçant $-\sqrt{-5}$ par $-\sqrt{5}$.

De plus

$$4+3\sqrt{-5}$$

$$= \left(\frac{5+\sqrt{-5}-(1-\sqrt{-5})\sqrt{-1}}{2}\right)\left(\frac{5-\sqrt{-5}-(1+\sqrt{-5})\sqrt{-1}}{2}\right)$$

$$= (5+\Omega+\Omega_1)(5-\Omega-S(\Omega_1)),$$

avec une décomposition semblable pour $4-3\sqrt{-5}$.

Prenons des exemples d'idéaux non principaux

$$(2, 1-\sqrt{-5}) = (2, 1+\sqrt{-5}, 1+\sqrt{-1}, 1-\sqrt{-1}) = (1+\sqrt{-1})$$

car

$$(2) = (1+\sqrt{-1})(1-\sqrt{-1}),$$

$$(1+\sqrt{5}) = (1+\sqrt{-1})(-2-S(\Omega)-\Omega_1),$$

de même

$$(3, 1+\sqrt{-5}) = (-2-S(\Omega)-\Omega_1),$$

$$(3, 1-\sqrt{-5}) = (3-\Omega-\Omega_1),$$

et de même

$$(7, 3+\sqrt{5}) = (4-2\Omega-3S(\Omega)-\Omega_1),$$

de plus

$(23, 8+\sqrt{-5}) = (8 -$ [illegible] $- \Omega + 3\Omega_1)$, etc.

En répétant plusieurs fois l'application de ce théorème on démontre qu'il est encore vrai lorsqu'on remplace le mot idéal premier par le mot idéal.

Enfin dans l'exemple $k(\sqrt{-5})$ nous pouvons montrer que le corps de classe a un nombre impair de classes.

Admettons que $\mathfrak{J}$ soit un idéal non principal du corps $K(\sqrt{-1})$ tel que $\mathfrak{J}^2 \sim 1$. Comme $\mathfrak{J}S(\mathfrak{J})$ est un idéal du corps fondamental et que par cela même il est un idéal principal de celui-ci ou du corps de classe, on aurait

$$\mathfrak{J}^2 \sim \mathfrak{J}S(\mathfrak{J})$$

ou

$$\mathfrak{J} \sim S(\mathfrak{J}).$$

Posons

$$B = \frac{\mathfrak{J}}{S(\mathfrak{J})}$$

on a

$$N_k(B) = \pm 1.$$

Dans le cas

$$N_k(B) = +1, \qquad B = \frac{S(A)}{A}.$$

et dans le cas

$$N_k(B) = -1$$

comme

$$N_k(E) = -1, \qquad EB = \frac{S(A)}{A}.$$

Dans les deux cas

$$(A)\mathfrak{J} = S(A\mathfrak{J}).$$

$(A)\mathfrak{J}$ serait donc un idéal du corps de base ou le produit d'un idéal ambige du corps de classe par un idéal du corps de base. Mais comme le discriminant du corps de classe n'a pas de facteur premier et que le corps de classe n'a pas d'idéal ambige, $A(\mathfrak{J})$ est un idéal du corps de base et par suite $\mathfrak{J} \sim 1$, c'est-à-dire que si le carré d'un idéal $\mathfrak{J}$ est un idéal principal, cet idéal $\mathfrak{J}$ est aussi un idéal principal.

Si donc le nombre des classes du corps relatif $H = 2^a u$, où u est un entier impair, on aurait pour tout idéal de la suite

$$\mathfrak{J}^{2^a u} \sim 1, \qquad \mathfrak{J}^{2^{a-1} u} \sim 1, \qquad \mathfrak{J} \sim 1,$$

ce qui est impossible. Le nombre des classes est impair.

On voit immédiatement que les considérations établies pour le corps $k(\sqrt{-5})$ s'appliquent presque littéralement à tout corps de base $k(\sqrt{m})$ ayant un nombre de classes égal à 2 et déterminé par un nombre premier négatif $m \equiv 3, (4)$. On peut choisir comme corps de classe d'un tel corps le corps relatif $K(\sqrt{-1})$; l'unité fondamentale ε_1 du corps $k(\sqrt{-m}) = k(\sqrt{-1}\sqrt{m})$ pour laquelle $n(\varepsilon_1) = -1$ est aussi une unité dans $K(\sqrt{-1})$ avec la norme relative -1.

Les théorèmes que nous venons d'établir dans l'exemple précédent sont vrais pour tout corps de base dont le nombre des classes est 2, comme M. Hilbert l'a démontré.

Si nous voulons nous en tenir à des corps de base quadratiques imaginaires $k(\sqrt{m})$ la condition $h = 2$ exige que le genre $g \leq 2$.

Mais on sait que $g = 2^{r-1}$ où r est le nombre des facteurs premiers distincts du discriminant du corps $k(\sqrt{m})$. Dans le cas où m satisfait à $m \equiv 1\ (4)$ et ne contient qu'un facteur premier, on a $r = 1$, $g = 1$, et le nombre des classes de $k(\sqrt{m})$ est impair. Pour $h = 2$ on ne peut avoir que $g = 2$, $r = 2$, c'est-à-dire que ou bien m est un nombre premier négatif de la forme $m \equiv 3\ (4)$ ce qui est le cas considéré, ou bien $m \equiv 2\ (4)$ ou $m \equiv 1\ (4)$, le nombre m contient dans le premier cas le facteur 2 et un autre facteur premier de la forme $4n \pm 3$, dans le second cas m contient un facteur premier rationnel positif $p \equiv 1\ (4)$ et un second facteur premier rationnel positif $q \equiv 3\ (4)$.

Quelques exemples pour montrer qu'on rencontre ces cas possibles.

2e *Exemple.* — Le corps $k(\sqrt{-22})$ a pour discriminant $d = -88$, le nombre des classes $h = 2$ et le genre $g = 2$. Soit $\mathfrak{p}$ un idéal premier avec 2, sans être un idéal principal, et posons $\pi = \mathfrak{p}^2$, la congruence $\pm\pi \equiv \alpha^2\ (4)$ est toujours satisfaite par un entier du corps soit pour $+\pi$ ou pour $-\pi$.

Car soit p le nombre premier rationnel qui contient $\mathfrak{p}$ et soit

$$\pi = a + b\sqrt{-22}, \qquad p^2 = \pi . \pi' = a^2 + 22b^2.$$

Comme $p^2 \equiv 1\ (4)$ il faut que a soit impair et que b soit pair, c'est pourquoi

$$\pm(a + b\sqrt{-22}) \equiv \alpha^2\ (4)$$

admet comme solution un entier du corps $k(\sqrt{-22})$. Soit $\pi_1 = \pm\pi$

le nombre pour lequel $\pi_1 \equiv \alpha^2 \ (4)$, le corps $K(\sqrt{\pi_1})$ représentera par rapport au corps de base $k(\sqrt{-22})$ un corps relatif dont le discriminant relatif ne contient pas d'idéal différent de ± 1.

Soit par exemple

$$\mathfrak{p} = (11, \sqrt{-22}), \qquad \mathfrak{p}^2 = 11,$$

$K(\sqrt{-11})$ est alors un corps de classe du corps de base $k(\sqrt{-22})$ pour lequel on a les théorèmes suivants :

Théorème 1. — Le discriminant relatif du corps $K(\sqrt{-11})$ par rapport au corps $k(\sqrt{-22})$ est une unité.

Tous les entiers du corps relatif peuvent être représentés au moyen des nombres de base

$$1, \quad \omega = \sqrt{-22}, \quad \Omega = 11\,\frac{11+\sqrt{-11}}{22}, \quad \Omega_1 = \sqrt{-22}\,\frac{11+\sqrt{-11}}{22}.$$

Comme le corps relatif contient tous les nombres du corps quadratiques $k(\sqrt{-11})$ et $k(\sqrt{2})$, on a en tenant compte du système des caractères des idéaux le

Théorème 2. — Tout idéal premier principal de $k(\sqrt{-22})$ se décompose dans $K(\sqrt{-11})$ en deux idéaux premiers distincts relativement conjugués.

Enfin pour les idéaux non principaux du corps $k(\sqrt{-22})$ on a le

Théorème 3. — Les idéaux premiers du corps de base $k(\sqrt{-22})$ qui n'appartiennent pas à la classe principale, sont encore des idéaux premiers du corps relatif $K(\sqrt{-11})$, mais ils y deviennent des idéaux principaux.

On voit tout d'abord que l'idéal $(11, \sqrt{-22})$ devient un idéal principal du corps relatif car

$$(11, \sqrt{-22}) = (\sqrt{-11}).$$

Soit maintenant $\mathfrak{p}$ un idéal non principal

$$(11, \sqrt{-22}) \cdot \mathfrak{p} = (\alpha)$$

est un idéal principal du corps de base

$$(11)\,\mathfrak{p}^2 = \alpha^2$$

ou

$$\mathfrak{p}^2 = \frac{(\alpha)^2 (\sqrt{-11})^2}{11^2}.$$

Mais d'autre part $\frac{\alpha\sqrt{-11}}{11}$ est un entier du corps relatif, c'est-à-dire que $\mathfrak{p}$ est un idéal principal de ce corps.

En tenant compte des trois premiers théorèmes on obtient le

Théorème 4. — Le nombre des classes du corps relatif $K(\sqrt{-11})$ est un nombre impair.

3ᵉ *Exemple*. — Soit le corps de base $k(\sqrt{-15})$ ou $-m = 3.5$, son discriminant $d = -15$, sa base 1, $\omega = \frac{1+\sqrt{-15}}{2}$, le nombre des classes et le genre sont égaux à 2.

Il en résulte que tous les nombres premiers rationnels p tels que $\left(\frac{-15}{p}\right) = +1$, $\left(\frac{p}{3}\right) = 1$, $\left(\frac{p}{5}\right) = 1$ se décompose dans $k(\sqrt{-15})$ en un produit de deux idéaux principaux.

Soit $\mathfrak{p}$ un idéal premier, premier avec 2, qui ne soit pas un idéal principal et soit $(\pi) = \mathfrak{p}^2$, on démontre encore que l'on peut satisfaire à $\pm\pi = \alpha^2$ (4).

Si l'on prend par exemple $\mathfrak{p} = (3, \sqrt{-15})$ ou $\mathfrak{p} = (5, \sqrt{-15})$ on trouve que les corps relatifs $K(\sqrt{-3})$, $K(\sqrt{5})$ sont des corps de classes par rapport au corps $k(\sqrt{-15})$ avec les propriétés établies dans les exemples précédents. Ces exemples donnent un aperçu très net des corps quadratiques imaginaires et des corps relatifs quadratiques. Le fait le plus curieux est l'existence de ce corps de classe dans lequel tous les idéaux non principaux des sous-corps deviennent des idéaux principaux.

Un corps de base réel se comporte d'une façon toute différente de celle d'un corps de base quadratique imaginaire.

Il nous faut d'abord définir une notion établie par M. Hilbert (d'après l'exemple de Gauss et de Dedekind) [1].

La notion de nombre totalement positif et primaire.

Définition. — Un nombre α du corps quadratique réel $k(\sqrt{m})$ est

---

[1] Voir Dedekind. — *Vorles. über Zahlentheorie von* Dirichlet *und* Dedekind. 4 Aufl., Suppl. XI, p. 578.

dit totalement positif, si α est un nombre positif ainsi que son conjugué α'. Soit de plus α un nombre totalement positif premier avec 2 et tel que $\alpha \equiv \nu^2$, (4), ν étant un entier de $k(\sqrt{m})$, α est dit un nombre primaire du corps $k(\sqrt{m})$.

Il nous sera ici plus utile de donner une autre idée de la condition d'équivalence.

Définition. — Deux idéaux $\mathfrak{j}$ et $\mathfrak{f}$ du corps $k(\sqrt{m})$ sont dits équivalents au sens restreint, si leur quotient $\frac{\mathfrak{j}}{\mathfrak{f}} = \alpha$, α étant un nombre totalement positif du corps k. Deux idéaux quelconques équivalents d'après cette définition appartiennent à la même classe d'idéaux.

La classe d'idéaux dans le sens restreint sera représentée par h.

Dans l'égalité $\frac{\mathfrak{j}}{\mathfrak{f}} = \alpha$, α n'est déterminé qu'à un facteur unité près. Il importe donc pour déterminer h de savoir si la norme de l'unité fondamentale du corps quadratique égale $+1$ ou -1.

En effet, soit ε une unité fondamentale positive de $k(\sqrt{m})$ et $n(\varepsilon) = +1$, ε' est aussi positif ou encore ε est totalement positif.

Le quotient défini par $\frac{\mathfrak{j}}{\mathfrak{f}} = \alpha$ est donc de prime abord totalement positif ou il ne l'est pas.

Dans ce cas chaque classe du corps primitif se décompose en deux nouvelles classes dans le sens restreint.

Car si α_1 est un nombre positif de norme négative, l'équivalence des deux idéaux $\mathfrak{j}$, $\mathfrak{f}$ au sens plus large, on déduit $\mathfrak{j} \dashv (\alpha_1)\mathfrak{f}$ au sens restreint, alors qu'au sens large $\mathfrak{f}$ et $(\alpha_1)\mathfrak{f}$ sont équivalents.

Si h est le nombre des classes au sens large, $\bar{h}$ le nombre des classes au sens restreint, on a $\bar{h} = 2h$.

$k(\sqrt{5})$,	$\varepsilon = \omega = \frac{1+\sqrt{5}}{2}$,	$n(\varepsilon) = -1$,	$h = 1$,	$\bar{h} = 1$,
$k(\sqrt{7})$,	$\varepsilon = 8 + 3\sqrt{7}$,	$n(\varepsilon) = +1$,	$h = 1$,	$\bar{h} = 2$,
$k(\sqrt{10})$,	$\varepsilon = 3 + \sqrt{10}$,	$n(\varepsilon) = -1$,	$h = 2$,	$\bar{h} = 2$,
$k(\sqrt{15})$,	$\varepsilon = 4 + \sqrt{15}$,	$n(\varepsilon) = +1$.	$h = 4$,	$\bar{h} = 4$.

On démontre d'une façon générale qu'à tout corps ayant un nombre de classes impaires $\bar{h}$ on ne peut superposer aucun surcorps non ramifié, tandis qu'il existe des surcorps non ramifiés pour tous

les autres corps. Pour un corps de $h = 2$ un pareil corps est aussi corps de classe avec des propriétés analogues aux corps de classe relatifs à des corps de base imaginaires et que nous avons appris à connaître.

Comme exemple particulier nous étudierons $k(\sqrt{5})$ qui a $h = h = 1$. S'il existait un surcorps relatif quadratique non ramifié et s'il était déterminé par le nombre μ de k, μ à part des facteurs carrés, ne pourrait contenir que des unités ou des diviseurs de 2.

Comme μ doit être premier avec 2, il ne nous reste plus qu'à voir si l'on peut poser $\mu = -1$ ou $\mu = \pm \omega$.

Dans le premier cas il faut voir si $\pm \omega \equiv \alpha^2 \ (4)$ est satisfaite pour un nombre du corps.

Soit

$$\alpha = x + y\omega, \qquad \alpha^2 = x^2 + y^2 + (2xy + y^2)\omega,$$

il s'agit de savoir si l'on peut satisfaire simultanément à

$$x^2 + y^2 \equiv 0 \ (4),$$
$$y^2 + 2xy \pm 1 \equiv 0 \ (4),$$

pour $+1$ ou -1 dans la dernière ligne par des valeurs entières et rationnelles de x et de y. On reconnaît sans peine que pour avoir

$$y^2 + 2xy - 1 \equiv 0 \ (4),$$

il faut que x soit pair et y impair, mais alors

$$x^2 + y^2 \equiv y^2 \not\equiv 0 \ (4).$$

De plus pour que

$$y^2 + 2xy + 1 \equiv 0 \ (4),$$

il faut que x et y soient impairs, et alors

$$x^2 + y^2 \equiv 2 \not\equiv 0 \ (4).$$

On arriverait au même résultat par un autre raisonnement qui convient au cas général :

Supposons qu'il existe une unité fondamentale ε telle que

$$\pm \varepsilon \equiv \alpha^2 \ (4).$$

on aurait aussi

$$\pm \varepsilon' \equiv \alpha'^2 \ (4)$$

et par suite

$$\varepsilon\varepsilon' \equiv (\alpha\alpha')^2 \ (4)$$

ou encore

$$(\alpha\alpha')^2 \equiv -1 \ (4).$$

Mais comme $\alpha\alpha'$ est toujours un entier rationnel, cette dernière congruence est impossible et l'hypothèse

$$\pm \varepsilon \equiv \alpha^2 \ (4)$$

n'est pas admissible.

Le corps $K(\sqrt{\pm\omega})$ n'est donc pas ramifié par rapport au corps $k(\sqrt{5})$, et le corps $K(\sqrt{-1})$ ne l'est pas davantage car on ne peut avoir

$$-1 \equiv \alpha^2 \ (4).$$

D'ailleurs d'une façon générale en vertu de $n(\varepsilon) = -1$ on a toujours

$$m \equiv 1 \ (4) \qquad \text{ou} \qquad m \equiv 2 \ (4),$$

c'est pourquoi la congruence $-1 \equiv \alpha^2$ (4) entraînerait toujours une congruence $-1 \equiv x^2$ (4) avec x entier et rationnel ; mais cette dernière est impossible.

D'autre part soit $k(\sqrt{m})$ un corps tel que $h = 1$ et par suite $\bar{h} = 2$, dont l'unité fondamentale ε a pour norme $+1$, il existe toujours un corps de classe qui lui correspond. Supposons $m \equiv 1$ ou $m \equiv 2$ (4) et ne contenant aucun facteur carré, posons $\varepsilon = \frac{\alpha}{\alpha'}$. On voit tout d'abord que $\varepsilon = \frac{1+\varepsilon}{1+\varepsilon'}$, mais on reconnaît facilement que l'on peut choisir $\alpha = \frac{1+\varepsilon}{t}$ de telle sorte que α et α' soient des entiers premiers avec 2. Il en résulte que $\varepsilon\alpha'^2 = \alpha\alpha'$, et comme $\alpha\alpha'$ est un entier rationnel impair on aura toujours

$$\pm \alpha\alpha' \equiv 1 \ (4),$$

c'est-à-dire que $\varepsilon\alpha'^2$ satisfait à

$$\pm \varepsilon\alpha'^2 \equiv \nu_1^2 \ (4).$$

Et comme on a supposé α' premier avec 2, il en résulte

$$\pm \varepsilon \equiv \nu^2 \ (4),$$

par suite $\mu = \pm \varepsilon$ détermine un corps quadratique relatif non ramifié. Un pareil corps est déjà déterminé par $\mu = -1$ lorsque $m \equiv 3 \ (4)$, car dans ce cas

$$-1 \equiv (\sqrt{m})^2 \ (4).$$

4e *Exemple*. — Corps de base $k(\sqrt{7})$. Ici

$$h = 1, \quad \varepsilon = 8 + 3\sqrt{7}, \quad n(\varepsilon) = +1, \quad h = 2.$$

Il y a deux classes d'idéaux au sens restreint ; les idéaux premiers $(3 \pm \sqrt{7})$, (5), (11), (13), (17), (23), $(6 \pm \sqrt{7})$, etc., appartiennent à la classe principale, les idéaux premiers $(3 \pm 2\sqrt{7})$, $(9 \pm 4\sqrt{7})$, $(4 \pm 3\sqrt{7})$, etc., appartiennent à la classe non principale.

Les idéaux premiers de la première classe sont ou bien des nombres premiers rationnels, ou bien ils ont été obtenus en décomposant en facteurs le nombre premier $p = 2$ et les nombres premiers de la forme $p \equiv 1 \ (4)$.

Pour les idéaux $\mathfrak{p}$ de la classe non principale on a dans le cas où l'on pose $\mathfrak{p}\mathfrak{p}' = p$, $p \equiv 3 \ (4)$.

Mais $-1 \equiv (\sqrt{7})^2 \ (4)$, $\mu = -1$ détermine par suite un corps relatif quadratique non ramifié. De plus soit $\mathfrak{p}$ un idéal premier de la classe non principale, et soit $(\pi) = \mathfrak{p}^2$, $\mu = \pm \pi$, d'après le théorème de M. Hilbert, détermine aussi un corps satisfaisant à cette condition.

Considérons $K(\sqrt{-1})$.

On peut prendre comme base de ce corps relatif

$$1, \quad \omega = \sqrt{7}, \quad \Omega = \frac{\sqrt{7} + \sqrt{-1}}{2}, \quad \Omega_1 = \sqrt{7}\,\frac{\sqrt{7} + \sqrt{-1}}{2},$$

$\varepsilon = 8 + 3\sqrt{7}$ est une unité du corps $k(\sqrt{7})$ et ε est la norme de

$$\mathrm{E} = \frac{(3 + \sqrt{7})(1 - \sqrt{-1})}{2}.$$

E est donc une unité du corps relatif.

Pour tout idéal premier de la première classe la congruence $-1 \equiv x^2 (\mathfrak{p})$ est possible, par contre elle est impossible pour les idéaux premiers de la seconde classe.

Les idéaux premiers de la première classe se décomposent dans le corps relatif en un produit de deux idéaux premiers, les idéaux premiers de la seconde classe demeurent des idéaux premiers dans le corps relatif.

Il est facile d'établir les décompositions suivantes pour les idéaux de la classe principale

$$(3 + \sqrt{7}) = (1 + \sqrt{-1})(5 + 2\omega - 3\Omega - \Omega_1),$$
$$(5) = (2 - \sqrt{-1})(2 - \sqrt{-1}) = (2 - \omega - 2\Omega)(2 + \omega - 2\Omega),$$
$$(11) = (2 + \sqrt{-7})(2 - \sqrt{-7}) = (-5 + 2\Omega_1)(9 - 2\Omega_1),$$
$$(13) = (3 + 2\sqrt{-1})(3 - 2\sqrt{-1}),$$
$$(17) = (4 + \sqrt{-1})(4 - \sqrt{-1}),$$
$$(23) = (4 + \sqrt{-7})(4 - \sqrt{-7}),$$
$$(6 + \sqrt{7}) = (3 + 2\omega - 3\Omega - \Omega_1)(3 + 2\omega - 3S(\Omega) - S(\Omega_1)), \text{ etc.}$$

Les idéaux premiers de la seconde classe demeurent des idéaux premiers, mais ils deviennent des idéaux principaux, car on peut écrire par exemple :

$$(3 + 2\sqrt{7}) = (3\sqrt{-1} - 2\sqrt{-7}).$$

De même que dans le cas du corps imaginaire on démontre que $K(\sqrt{-1})$ possède un nombre impair de classes au sens restreint.

Le corps $K(\sqrt{-1})$ est encore un corps de classe de $k(\sqrt{7})$, de même que le corps $K(\pm\sqrt{7})$ dont il a été question précédemment, car ces corps possèdent les propriétés caractéristiques d'un corps de classe.

Pour l'autre cas où $m \equiv 2\ (4)$ il suffit d'indiquer l'exemple $k(\sqrt{6})$. Comme

$$h = 1 \quad , \quad \varepsilon = 5 - 2\sqrt{6} \quad , \quad n(\varepsilon) = +1$$

par suite $\bar{h} = 2$ il existe des corps de classes relativement quadratiques non ramifiés. On voit en effet que

$$K(\sqrt{-5 + 2\sqrt{6}}) = K(\sqrt{-\varepsilon})$$

est un pareil corps relatif.

Un dernier exemple nous montrera ce qui se passe pour un corps tel que $h = h = 2$. Je me contenterai de citer des résultats et de renvoyer à la note de M. Hilbert.

5ᵉ *Exemple*. — Corps de base $k(\sqrt{10})$ avec $h = h = 2$. Soit un idéal premier quelconque premier avec 2 et qui n'appartient pas à la classe principale, par exemple

$$\mathfrak{p} = (3, 2 - \sqrt{10}).$$

Soit

$$(\pi) = \mathfrak{p}^2 = (-1 - \sqrt{10}).$$

Désignons par ε l'unité fondamentale du corps, il résulte des théorèmes généraux de M. Hilbert que l'une des deux congruences $\pm \varepsilon\pi \equiv \alpha^2 \ (4)$ est toujours satisfaite par un entier α du corps $k(\sqrt{10})$. Et en effet

$$\mu = \varepsilon\pi = 7 - 2\sqrt{10} \equiv (1 - \sqrt{10})^2 \ (4).$$

Il en résulte que $K(\sqrt{7 + 2\sqrt{10}})$ est par rapport à $k(\sqrt{10})$ un corps relatif quadratique non ramifié. On peut choisir comme base de ce corps relatif

$$1,\quad \omega = \sqrt{10},\quad \Omega = \frac{3(1 - \sqrt{10}) + \sqrt{\mu}}{2},\quad \Omega_1 = (2 - \sqrt{10})\frac{3(1 - \sqrt{10}) - \sqrt{\mu}}{6}.$$

De plus

$$E = \frac{1 - \sqrt{10} + \sqrt{\mu}}{2} \quad \text{et} \quad H = 1 - E$$

sont des unités dans $K(\sqrt{\mu})$ avec

$$N_k(E) = 1, \quad N_k(H) = 3 + \sqrt{10} = \varepsilon.$$

Voyons si $(3, 2 - \sqrt{10})$ n'est pas un idéal principal du corps $K(\sqrt{\mu})$. On voit facilement que

$$(3) = (\sqrt{\mu})(20 - 4\omega - \Omega - 5\Omega_1) = \sqrt{\mu}\,(\mathbf{A}_1)$$

$$(2 + \sqrt{10}) = (\sqrt{\mu})(34 - 11\omega - 4\Omega - 10\Omega_1) = \sqrt{\mu}\,(\mathbf{B})$$

et que

$$(3, 2 + \sqrt{10}) = (\sqrt{\mu}).$$

Les décompositions de 3 et de $2 + \sqrt{10}$ nous montrent que $(2, \sqrt{10}) = (\mathrm{B})$ et que $(2) = (\mathrm{B})^2$.

D'où il résulte de plus que

$$(\sqrt{10}) = (\mathrm{B})(25 + 7\omega - 6\Omega + 4\Omega_1) = (\mathrm{B})(\mathrm{B}_1)$$
$$(5) = (3 - \sqrt{10})^2 (\mathrm{B}_1)^2 = (\Gamma)^2$$

où

$$\Gamma = (25 + 7\omega - 6\Omega + 4\Omega_1)(3 - \sqrt{10}).$$

A l'aide des égalités numériques

$$2 = \mathrm{B}^2 \quad \text{et} \quad 5 = \Gamma^2$$

il nous est facile d'expliquer les lois de décomposition du corps relatif.

Soit (p) un idéal principal du corps $k(\sqrt{10})$,

$$\left(\frac{10}{p}\right) = -1$$

condition remplie lorsque

$$\left(\frac{2}{p}\right) = +1, \quad \left(\frac{5}{p}\right) = -1$$

ou lorsque

$$\left(\frac{2}{p}\right) = -1, \quad \left(\frac{5}{p}\right) = +1.$$

Mais alors l'une des deux équations

$$p = x^2 - 2y^2$$
$$p = x^2 - 5y^2$$

admet des solutions entières rationnelles, ou encore on a dans le corps relatif l'une des décompositions :

$$(p) = (x - \mathrm{B}y)(x + \mathrm{B}y)$$

ou

$$(p) = (x - \Gamma y)(x + \Gamma y).$$

On a par exemple :

$$7 = 3^2 - 2.1^2, \qquad (7) = (3 - \mathrm{B})(3 + \mathrm{B})$$
$$11 = 16 - 5, \qquad (11) = (4 - \Gamma)(4 + \Gamma)$$
$$17 = 5^2 - 2.2^2, \qquad (17) = (5 - 2\mathrm{B})(5 + 2\mathrm{B})$$
$$19 = 12^2 - 5.5^2, \qquad (19) = (12 - 5\Gamma)(12 + 5\Gamma)$$

Si p désigne un nombre premier qui se décompose parce que

$$\left(\frac{10}{p}\right) = +1$$

il y a deux cas à considérer suivant que

$$\left(\frac{2}{p}\right) = +1, \quad \left(\frac{5}{p}\right) = +1$$

ou que

$$\left(\frac{2}{p}\right) = -1, \quad \left(\frac{5}{p}\right) = -1.$$

Dans le premier cas p se décompose dans le corps $k(\sqrt{10})$ en un produit de deux idéaux principaux car le corps $k(\sqrt{10})$ admet deux genres contenant chacun une classe, et les facteurs de (p) appartiennent à la classe principale. On a donc

$$(p) = (x + \sqrt{10}\,y)(x - \sqrt{10}\,y).$$

Mais comme on a aussi

$$(p) = x^2 - 2y^2 \quad \text{et} \quad p = x_1^2 - 5y_1^2$$

p dans le corps relatif se décompose en un produit de quatre idéaux distincts. Chacun des idéaux principaux

$$x + \sqrt{10}\,y, \quad x - \sqrt{10}\,y$$

est donc le produit de deux idéaux premiers du corps relatif.

Voyons des exemples, les nombres premiers p, pour lesquels

$$\left(\frac{2}{p}\right) = +1, \quad \left(\frac{5}{p}\right) = +1$$

sont de la forme

$$40n \pm 1, \quad 40n \pm 9$$

$$31 = 11^2 - 10.3^2 = (11 - 3\sqrt{10})(11 + 3\sqrt{10}) = \mathfrak{p}' . \mathfrak{p}$$

$$\mu \equiv 4, (\mathfrak{p}'), \quad \mu \equiv 14^2. (\mathfrak{p})$$

$$\frac{11 - 3\sqrt{10}}{3 - \sqrt{10}} = (2 - \sqrt{\mu})(2 + \sqrt{\mu}).$$

On a donc l'égalité idéale

$$(11 - 3\sqrt{10}) = (2 - \sqrt{\mu})(2 + \sqrt{\mu})$$

et de plus

$$(11 + 3\sqrt{10}) = \left(-1 + \sqrt{10} + 2\,\frac{(2 - \sqrt{10})\sqrt{\mu}}{3}\right)$$
$$\left(-1 + \sqrt{10} - 2\,\frac{(2 - \sqrt{10})\sqrt{\mu}}{3}\right).$$

De plus

$$41 = 9^2 - 10.2^2 = (9 - 2\sqrt{10})(9 + 2\sqrt{10}) = \mathfrak{p}.\mathfrak{p}'$$
$$\mu \equiv 4^2, (\mathfrak{p}) \qquad \text{et} \qquad \mu \equiv 11^2, (\mathfrak{p})$$

et

$$(9 - 2\sqrt{10}) = (4 - \sqrt{\mu})(4 + \sqrt{\mu})$$
$$(9 + 2\sqrt{10}) = \left(8 + 2\sqrt{10} + \frac{(5 + 2\sqrt{10})\sqrt{\mu}}{3}\right)$$
$$\left(8 + 2\sqrt{10} - \frac{(5 + 2\sqrt{10})\sqrt{\mu}}{3}\right).$$

On a aussi

$$79 = 13^2 - 10.3^2 = (13 - 3\sqrt{10})\,(13 + 3\sqrt{10}) = \mathfrak{p}'.\mathfrak{p}$$
$$\mu \equiv 11^2, (\mathfrak{p}'), \qquad \mu \equiv 29^2, (\mathfrak{p})$$
$$(13 - 3\sqrt{10}) = \left(-2 + \sqrt{10} + \frac{(-5 + \sqrt{10})\sqrt{\mu}}{3}\right)$$
$$\left(-2 + \sqrt{10} - \frac{(5 - \sqrt{10})\sqrt{\mu}}{3}\right).$$
$$(13 + 3\sqrt{10}) = \left(-2 + \sqrt{10} + \frac{(5 - \sqrt{10})\sqrt{\mu}}{3}\right)$$
$$\left(-2 + \sqrt{10} - \frac{(5 - \sqrt{10})\sqrt{\mu}}{3}\right).$$

Enfin

$$89 = 27^2 - 10.8^2 = (27 - 8\sqrt{10})(27 + 8\sqrt{10}) = \mathfrak{p}'.\mathfrak{p}$$
$$\mu \equiv 6^2\,(\mathfrak{p}'), \qquad \mu \equiv 44^2, (\mathfrak{p})$$
$$(27 - 8\sqrt{10}) = \left(1 + 2\,\frac{(7 - 2\sqrt{10})\sqrt{\mu}}{3}\right)\left(1 - 2\,\frac{(7 - 2\sqrt{10})\sqrt{\mu}}{3}\right)$$
$$(27 + 8\sqrt{10}) = (1 + 2\sqrt{\mu})(1 - 2\sqrt{\mu})$$

Nous nous contenterons de ces exemples et nous allons voir ce qui se passe pour les idéaux (p) du corps de base lorsqu'on a simultanément

$$\left(\frac{2}{p}\right) = -1, \quad \left(\frac{5}{p}\right) = -1.$$

Dans ce cas les facteurs premiers de (p) n'appartiennent ni au genre principal ni à la classe principale.

Mais comme dans ce cas l'équation

$$p = 2x^2 - 5y^2$$

admet toujours des solutions entières et rationnelles, (p) admettra dans le corps relatif les décompositions

$$(p) = (\mathrm{B}x + \Gamma y)(\mathrm{B}x - \Gamma y)$$

et nous avons déjà vu que les idéaux $(2, \sqrt{10})$ $(5, \sqrt{10})$ deviennent des idéaux principaux

$$\left(\frac{10}{13}\right) = +1, \quad \left(\frac{2}{13}\right) = -1, \quad \left(\frac{5}{13}\right) = -1$$

$$(13) = (13, 6 - \sqrt{10})(13, 6 + \sqrt{10}) = \mathfrak{p}' \, \mathfrak{p}.$$

Aucun nombre entier du corps $k\sqrt{10}$ ne satisfait

$$\mu \equiv \alpha^2, (\mathfrak{p}) \quad \text{ou} \quad \mu \equiv \alpha^2, (\mathfrak{p}').$$

En effet

$$\mu \equiv 8, (\mathfrak{p}) \quad \text{et} \quad \mu \equiv 6, (\mathfrak{p}').$$

C'est-à-dire que $\mathfrak{p}$ et $\mathfrak{p}'$ ne se décomposent pas dans le corps relatif. Mais on a dans le corps relatif

$$(13, 6 + \sqrt{10}) = (3\,\mathrm{B} + \Gamma), \quad (13, 6 - \sqrt{10}) = (3\,\mathrm{B} - \Gamma)$$

correspondant à $13 = 2 \cdot 9 - 5$.

De même

$$(37) = (37, 11 - \sqrt{10})(37, 11 + \sqrt{10}) = \mathfrak{p}' \, \mathfrak{p}$$

$$\mu \equiv 22, (\mathfrak{p}), \quad \mu \equiv 29, (\mathfrak{p}')$$

et dans le corps relatif

$$\mathfrak{p} = \mathfrak{P} = (9\mathrm{B} + 5\,\Gamma) \quad \mathfrak{p}' = \mathfrak{P}_1 = (9\mathrm{B} - 5\,\Gamma).$$

Les idéaux premiers du corps de base qui ne sont pas des idéaux principaux, demeurent des idéaux premiers dans $K(\sqrt{\mu})$ mais ils deviennent idéaux principaux.

De même que pour le corps imaginaire on démontre que le nombre des classes du corps relatif $K(\sqrt{\mu})$ est impair.

Et c'est ce fait que le nombre des classes du corps de classe est impair qui permet d'établir le théorème de réciprocité quadratique dans le corps de base.

On peut généraliser les théorèmes simples relatifs à l'existence de corps de classe pour des corps quadratiques lorsqu'on considère des corps relatifs du quatrième degré ou d'un degré supérieur.

Considérons par exemple le corps de base $k\sqrt{-14}$ qui a un nombre de classes $h = 4$.

On peut représenter les classes de ce corps par

$$(1), \; (2, \sqrt{-14}), \quad (3, 1 - \sqrt{-14}), \quad (3, 1 + \sqrt{-14}) = (\mathfrak{r})$$

ou

$$\mathfrak{r}, \mathfrak{r}^2, \mathfrak{r}^3, \mathfrak{r}^4 \sim 1.$$

Si l'on pose

$$(\rho) = \mathfrak{r}^4 = (5 - 2\sqrt{-14})$$

on vérifie facilement que

$$-\rho = -5 - 2\sqrt{-14} \equiv (1 + \sqrt{-14})^2, \; (4)$$

et on en déduit que

$$K\sqrt{-5 - 2\sqrt{-14}}$$

est un corps relatif quadratique non ramifié de $k(\sqrt{-14})$. Les nombres

$$1, \quad \omega = \sqrt{-14}, \quad \Omega = 9\,\frac{9(1 + \sqrt{-14}) + \sqrt{\mu}}{18}$$

$$\Omega_1 = (2 + \sqrt{-14})\,\frac{9(1 + \sqrt{-14}) + \sqrt{\mu}}{18}$$

forment une base de ce corps, et l'on reconnaît que les idéaux

$$\mathfrak{p}_2 = (2, \sqrt{-14}), \quad \mathfrak{p}_3 = \mathfrak{r} = (3, 1 - \sqrt{-14})$$

$$\mathfrak{p}'_3 = \mathfrak{r}' = (3, 1 - \sqrt{14})$$

ne se décomposent pas dans le corps relatif

$$\mathfrak{p}_2 = \mathfrak{P} = (12 - 3\sqrt{-14} + 2\Omega_1)$$

$$\mathfrak{r}^2 = (\sqrt{\mu})$$

deviennent des idéaux principaux, par contre $\mathfrak{r}$ et $\mathfrak{r}$ sont des idéaux non principaux du corps relatif. Il en résulte que le nombre des classes du corps relatif est encore pair. Pour atteindre le corps de classe de $k(\sqrt{-14})$ il faudrait choisir un sur-corps qui serait du quatrième degré par rapport à $k(\sqrt{-14})$.

Ces recherches nous conduiraient loin au delà du cadre de ce livre.

EXPLICATION DES TABLES

REMARQUES SUR LA RÉSOLUTION DE L'ÉQUATION DE PELL.

De même que la géométrie descriptive est un complément des théories abstraites de la géométrie, le calcul numérique est une application de la théorie des nombres. Ce calcul offre à celui qui a étudié les théories un attrait comparable à celui qu'offre le dessin de formes géométriques ou la représentation imagée de vérités géométriques.

De plus, celui qui étudie la théorie des nombres ne saura s'il en possède bien les notions qu'en les appliquant à des exemples, celui qui la possède déjà trouvera souvent dans ce calcul des sujets de recherche, les théorèmes les plus importants de la théorie des nombres n'ont-ils pas été découverts par voie d'induction.

Les tables qui terminent ce livre faciliteront certains calculs et permettront d'en vérifier d'autres. Ces tables indiquent aussi les nombres des classes des corps quadratiques dont le nombre fondamental sans facteur carré est compris entre — 97 et + 101.

La disposition des tables sera comprise sans autre explication. Elles sont divisées en deux parties, l'une pour les corps imaginaires, l'autre pour les corps réels.

Les colonnes verticales successives dans la table destinée aux corps imaginaires, contiennent dans l'ordre :

1° Le nombre fondamental du corps ;

2° La base la plus simple du corps ;

3° Le discriminant du corps, décomposé en ses facteurs premiers rangés par ordre de grandeur croissante ;

4° Tous les idéaux du corps non équivalents entre eux et dont la norme $< |\sqrt{d}|$.

5° L'énumération des classes représentées sous K^k, L^l, ... au

moyen du plus petit nombre possible de classes fondamentales.

La lettre A indiquera que la classe est ambige. Lorsque toutes les classes d'un corps peuvent être représentées par les puissances successives d'une seule classe J ou A, le corps est dit cyclique.

Les corps non cycliques de la table sont des corps abéliens. Toutes leurs classes peuvent être représentées par les puissances et les produits de deux classes choisies d'une façon appropriée.

On trouvera facilement dans les tables les classes ambiges autres que celles désignées par A ; ce sont celles dont le carré fournit la classe principale.

Les idéaux correspondent aux classes écrites sur la même ligne, l'idéal peut toujours être pris pour représenter la classe ;

6° La division des classes en genres ; les classes qui appartiennent à un même genre sont reliées par une accolade ;

7° Les systèmes de caractères des genres. D'après le n° 28 on sait que tout système de caractères se compose d'un certain nombre d'unités positives ou négatives $+1$, -1. Dans les tables nous n'écrirons que $+$, $-$ et ces signes se rapportent de gauche à droite aux facteurs premiers du discriminant écrits dans l'ordre croissant de gauche à droite dans la troisième colonne.

Dans la partie concernant les corps réels, il faut à ces colonnes en ajouter deux autres : la colonne des ε contient l'unité fondamentale du corps telle que $|\varepsilon| > 1$, et la colonne des $n(\varepsilon)$ en contient la norme.

De plus le calcul des systèmes de caractères diffère de ce qu'il était précédemment. Si m un nombre positif qui admet des diviseurs premiers de la forme $q \equiv 3\ (4)$, on a

$$\left(\frac{-1,\ m}{q}\right) = -1.$$

Soit alors $\mathfrak{j}$ un idéal du corps, nous choisirons $\bar{n} = \pm n(\mathfrak{j})$, tel que pour un facteur bien déterminé parmi ces q le symbole

$$\left(\frac{\bar{n},\ m}{q}\right) = +1.$$

C'est pourquoi lorsqu'on énumérera les caractère d'un idéal $\mathfrak{j}$ il suffira de considérer les facteurs premiers de d autres que q.

Et alors dans la troisième colonne les facteurs premiers de d sont

écrits dans l'ordre suivant, d'abord le nombre $q \equiv 3$ (4) employé pour fixer le signe de $\bar{n} = \pm n(\mathfrak{j})$, puis les autres facteurs dans l'ordre de grandeur croissante.

La colonne des systèmes de caractères donne les valeurs de $\left(\frac{\bar{n}, m}{p}\right)$, pour les facteurs premiers rangés comme nous l'avons dit, abstraction faite du facteur q.

Le calcul des tables est très simple, car on a vite une vue d'ensemble sur les points importants et l'on est amené à des artifices utiles.

Pour trouver les idéaux on cherche d'abord la valeur du symbole $\left(\frac{d}{p}\right)$ pour tous les nombres premiers $p < |\sqrt{d}|$ et l'on met les idéaux trouvés $\mathfrak{p}$, $\mathfrak{p}'$, etc., sous la forme $(p, a + \omega)$.

Pour reconnaître si les deux idéaux $\mathfrak{j}$ et $\mathfrak{h}$ contenus dans i et h sont équivalents, on forme $\mathfrak{j}'\mathfrak{h}$ et l'on voit s'il est un idéal principal. Tous les nombres de cet idéal ont alors un facteur commun ; on peut encore rechercher si

$$ih = x^2 - my^2 \qquad \text{ou} \qquad \pm ih = x^2 + xy + \frac{1 - m}{4} y^2,$$

suivant les cas, admet une solution entière en x et y. Cette façon d'opérer est très facile pour les corps imaginaires. Dans les corps réels on simplifie ce procédé en choisissant d'abord x et y et on cherche les nombres les plus petits a pour lesquels $x^2 - my^2 = a$, etc.

On peut souvent appliquer les théorèmes relatifs aux genres des corps pour décider si un idéal donné est idéal principal ou non. Nous l'avons montré sur des exemples au n° 55.

La détermination de l'unité fondamentale ε conduit à un problème analogue.

Il s'agit alors de résoudre une équation de la forme

$$x^2 - my^2 = 1 \qquad \text{ou} \qquad x^2 + xy + \frac{1 - m}{4} y^2 = \pm 1,$$

m étant positif.

Nous avons déjà indiqué précédemment les méthodes employées.

La méthode générale qui s'applique toujours est fondée sur le développement de $\sqrt{m}$ en fraction continue.

Mais dans bien des cas on peut utiliser les théorèmes sur les

genres et leurs conséquences (n° 32), ainsi que les propriétés des idéaux ambiges, comme on le verra d'après des exemples.

1° $k(\sqrt{55})$. D'après les notations antérieures $p(144)$, $t = 3$, $r = 2$ et par suite $q = 2$. Le corps contient deux classes ambiges. Les idéaux provenant de la décomposition de 2, 5, 10, 11 se répartissent dans ces deux classes. Comme l'idéal (2) se décompose et que la congruence

$$x^2 \pm 2 \equiv 0, (55),$$

il en résulte que

$$(2, 1 + \sqrt{55})$$

est un idéal ambige.

De plus comme

$$x^2 \pm 10 \equiv 0 (55$$

est impossible, les idéaux premiers contenus dans les idéaux (2) et (5) ne sont pas équivalents. L'idéal ambige obtenu en décomposant 5 est donc un idéal principal, ou encore (5) est le carré d'un idéal principal. Et en effet

$$5 = 15^2 - 55 . 4.$$

15 et 2 sont les plus petites solutions en valeur absolue de

$$5 = x^2 - 55y^2.$$

D'autre part comme 5 est le carré d'un idéal ambige

$$(5) = (15 \pm 2\sqrt{55})^2.$$

Et par suite en prenant le signe +

$$(5) = (5)(89 + 12\sqrt{55}).$$

$$\varepsilon = 89 + 12\sqrt{55}.$$

est une unité fondamentale du corps.

2° $k(\sqrt{31})$. 2 est contenu dans d, c'est-à-dire $2 = \mathfrak{p}^2$.

Mais on a montré précédemment que

$$2 = x^2 - 31y^2$$

admet des solutions. La congruence

$$x^2 - 2 \equiv 0, \ (31)$$

nous montre qu'alors

$$x = 8 + 31\,u \qquad \text{et} \qquad y^2 = 2 + 16u + 31\,u^2,$$

où u est un entier rationnel.

Il faut donc trouver u tel que la valeur de y^2 soit un carré parfait. On voit sans peine que

$$y^2 = 49 = 7^2 \qquad \text{pour} \qquad u = 1$$

et par suite $x = 39$.

Il en résulte

$$\mathfrak{p}^2 = (39 + 7\sqrt{31}),$$
$$(2) = (1521 - 1519,\ 2 \cdot 273\sqrt{31}) = \mathfrak{p}^2,$$
$$(2) = (2)\,(1520 + 273\sqrt{31}).$$

L'unité cherchée est

$$\varepsilon = 1520 + 273\sqrt{31}\,.$$

3° $k(\sqrt{67})$. La décomposition de 2 nous donne un idéal principal ambige, car le corps ne possède qu'une classe ambige, la principale. L'équation indéterminée

$$-2 = x^2 - 67y^2$$

admet des solutions.

$$x^2 + 2 \equiv 0 \ (67)$$

nous donne

$$x = 20 + 67u,$$
$$y^2 = 6 + 4u + 67u^2,$$

cette dernière est satisfaite pour $u = 3$

$$(2) = (221 + 27\sqrt{67})^2$$

et par suite

$$\varepsilon = 48842 + 5967\sqrt{67}\,.$$

4° $k(\sqrt{93})$. Dans ce corps $(3) = \mathfrak{p}_3^2$, et comme il n'y a qu'une classe, $\mathfrak{p}_3$ est un idéal principal. On voit rapidement que

$$(3) = (4 + \omega)(4 + \omega'),$$
$$(3) = (4 + \omega)^2,$$

d'où l'on tire

$$\varepsilon = 13 + 3\omega.$$

Les tables nous montrent que $k(\sqrt{94})$ est le corps dont l'unité fondamentale contient les plus grands nombres 2 143 295 et 221 064.

On détermine ces nombres assez rapidement en remarquant que $2 = x^2 - 94y^2$ doit admettre des solutions. Ici encore $(2) = (\alpha)^2$, et on en déduit ε comme précédemment.

Dans tous les exemples que nous avons considérés on arrive à résoudre soit

$$(1) \qquad x^2 - my^2 = 1 \qquad \text{soit} \qquad x^2 + xy + \frac{1-m}{4}y^2 = \pm 1$$

de la manière suivante : on cherche d'abord un idéal principal ambige du corps différent de $\sqrt{m}$ et du carré de cet idéal ambige on déduit ε. Cela revient à dire qu'on déduit les solutions de (1) des solutions de

$$x^2 - my^2 = \pm a,$$
$$x^2 + xy + \frac{1-m^2}{4}y^2 = \pm a,$$

où a est un facteur de $4m$ ou de m, lesquelles sont toujours plus petites que les solutions cherchées.

Ce procédé nous est interdit pour les cas comme $k(\sqrt{73})$, $k(\sqrt{97})$, ... où le nombre fondamental est un nombre premier de la forme $m \equiv 1\ (4)$, ou pour $k(\sqrt{65})$, $k(\sqrt{85})$, ... qui ne contiennent que $(\sqrt{73})$, $(\sqrt{97})$, $(\sqrt{65})$, $(\sqrt{95})$, c'est-à-dire $\sqrt{m}$ comme idéal principal ambige.

Supposons que dans le cas où m est premier on ait constaté que (a) est le produit de deux idéaux principaux conjugués, il est possible de déterminer les plus petits nombres α, α_1 tels que

$$+a = \alpha \cdot \alpha' \qquad \text{et} \qquad -a = \alpha_1 \cdot \alpha_1',$$

alors

$$n(\varepsilon) = -1,$$

et alors

$$\varepsilon = \frac{\alpha}{\alpha_1} \quad \text{ou} \quad \varepsilon = \frac{\alpha}{\alpha'_1}.$$

Dans $k(\sqrt{97})$

$$+2 = (38 - 7\omega)(38 - 7\omega'),$$
$$-2 = (146 - 33\omega)(146 - 33\omega'),$$
$$\varepsilon = \frac{146 - 33\omega}{38 - 7\omega} = 5035 - 1138\omega.$$

Pour les corps $k(\sqrt{65})$ et $k(\sqrt{85})$, le calcul de ε est facilité car on sait que $n(\varepsilon) = -1$.

On peut presque toujours abréger des calculs un peu longs par de petits raisonnements. La théorie générale fournit presque toujours un moyen de simplifier les calculs, et elle remplit ainsi un service qui est au fond le but de toute théorie générale.

INDEX

OUVRAGES CONTENANT DES TABLES NUMÉRIQUES

Répondant à une demande orale, je donne ici quelques indications quoique incomplètes de tables numériques.

D'abord on trouve dans toutes les tables de facteurs, comme en contiennent bien des tables de logarithmes, le moyen de reconnaître si un nombre est premier.

1. La plus grande de ces tables est celle de J. Ch. Burckhardt (*Table des diviseurs des nombres de* 1 *à* 3036000), Paris, 1814, 1816, 1817. — Celle de B. Goldberg, Leipzig, 1862, est plus petite (*Table des nombres premiers et des facteurs* de 1 *à* 251647.)

Les tables calculées par Ostrogradsky, Jacobi, etc., servent au calcul des nombres primitifs et des indices.

C. G. Jacobi, Canon *arithmeticus sive tabulæ quibus exhibentur pro singulis numeris primis vel primorum potestatibus infra* 1000 *numeri ad datos indices et indices ad datos numeros pertinentes* Berolini, 1839.

La théorie des congruences de Tschebyscheff contient un extrait de ces tables.

Legendre, Gauss, Degen, Jacobi et Cayley, ont calculé des tables relatives à la théorie des formes quadratiques et cubiques.

2. Il vient d'en être publié une nouvelle sous les auspices de M. Carnegie, par les soins de M. Lehmer pour tous les nombres de 1 à 10 000 000.

La théorie des nombres de Legendre, tome I, renferme 10 tables.

1 et 2. Les expressions les plus simples de

$$Ly^2 + 2Myz + Nz^2 \quad \text{et} \quad Ly^2 + Myz + Nz^2$$

pour toutes les valeurs non carrées de $A = M^2 - LN$ de $A = 2$ à $A = 136$ et de $B = M^2 - 4LN$ de $B = 5$ à $B = 305$.

3-8. Les diviseurs carrés et les diviseurs impairs de $t^2 \mp au^2$, $t^2 + 2au^2$.

10. Les plus petites valeurs de x et de y, qui satisfont à $x^2 - ny^2 = \pm 1$ pour toute valeur $N = 2$ à $N = 1003$, qui n'est pas un carré. (Comparer Degen et Tschebyscheff.)

C. F. Degen. Canon *Pellianus sive tabula simplissimam æquationis celebratissimæ* $y^2 = ax^2 + 1$ *solutionem, pro singulis numeri dati valoribus ab* 1 *usque aod* 1000 *in numeris rationalibus iidemque integris exhibens.* Havniæ 1817.

Ces tables sont très appréciées. Elles ont été calculées par la méthode des fractions continues. L'auteur a cependant indiqué un certain nombre de cas particuliers remarquables où les solutions sont immédiates.

C. F. Gauss. *Œuvres*, t. II. (Tiré des œuvres posthumes).

Table des caractères quadratiques des nombres premiers.

Table du nombre des classes de formes quadratiques linéaires.

Dans le complément à la première édition on trouve une Table des indices des nombres premiers dans le domaine supérieur, (c'est-à-dire des nombres de la forme $a + b\sqrt{-1}$).

Tables donnant des solutions de $A = fx^2 + gy^2$.

C. G. Jacobi. *Œuvres complètes*, t. VI.

Table donnant la décomposition de nombres premiers en sommes de la forme

$$a^2 + b^2, \quad a^2 + 2b^2, \quad a^2 + 3b^2.$$

Table indiquant le plus petit nombre de cubes dont sont composés les nombres jusqu'à 12000.

A. Cayley. *Collected papers*, vol. V, Cambridge 1892, p. 141-156

Tables des formes quadratiques linéaires pour les déterminants négatifs depuis $D = -1$ jusqu'à $D = -100$, pour les déterminants positifs non carrés depuis $D = 2$ jusqu'à $D = 99$ et pour les treize déterminants irréguliers qui se trouvent dans le premier mille.

Il y a peu d'œuvres de calcul numérique relatif aux nombres algébriques. Toutefois on trouve des résultats variés dans les *Dissertations* de Göttingen que nous avons citées et due à M. L.-W.

Reid à M.G. Rückle et de plus dans l'ouvrage de M.K.-S. Hilbert *Das allgemeine quadratische Reziprozitätsgesetz in ausgewählten Kreiskörpern der 2^h ten Einheitswüzeln.* Göttingen, 1900.

L. Sapolsky. Ueber die Theorie der relativ. abelchen kubischen Zahlkörper. Göttingen, 1902.

Les tables de C. G. Reuschle calculées d'après les prescriptions de Kummer, sont très riches en contenu et fort utiles :

Tafeln Komplexer Primzahlem, welche aus Wurzeln der Einheit Gebildet sind, Berlin, 1875.

TABLES

CORPS IMAGINAIRES

	Base 1 ω	d	Idéaux	Classes	Genres	Systèmes de caractères
-1 *)	$\sqrt{-1}$	-2^2	(1)	1	1	+
-2	$\sqrt{-2}$	-2^3	(1)	1	1	+
-3 **)	$\frac{1+\sqrt{-3}}{2}$	-3	(1)	1	1	+
-5	$\sqrt{-5}$	$-2^2 \cdot 5$	(1)	A^2	A^2	+ +
			$(2, 1+\sqrt{-5})$	A	A	− −
-6	$\sqrt{-6}$	$-2^3 \cdot 3$	(1)	A^2	A^2	+ +
			$(2, \sqrt{-6})$	A	A	− −
-7	$\frac{1+\sqrt{-7}}{2}$	-7	(1)	1	1	+
-10	$\sqrt{-10}$	$-2^3 \cdot 5$	(1)	A^2	A^2	+ +
			$(2, \sqrt{-10})$	A	A	− −
-11	$\frac{1+\sqrt{-11}}{2}$	-11	(1)	1	1	+
-13	$\sqrt{-13}$	$-2^2 \cdot 13$	(1)	A^2	A^2	+ +
			$(2, 1+\sqrt{-13})$	A	A	− −
-14	$\sqrt{-14}$	$-2^3 \cdot 7$	(1)	J^4	J^4 ***)	+ +
			$(3, 1-\sqrt{-14})$	J^3	J^2	
			$(2, \sqrt{-14})$	J^2	J^3	− −
			$(3, 1+\sqrt{-14})$	J	J	

* Ce corps contient outre ± 1 les unités $\pm \sqrt{-1}$.

** Ce corps contient en plus de ± 1 les unités $\pm \omega \pm \omega'$.

	Base 1 ω	d	Idéaux	Classes	Genres	Systèmes de caractères
-15	$\frac{1+\sqrt{-15}}{2}$	$-3 \cdot 5$	(1)	A^2	A^2	$+ \ +$
			$(2,\ 1+\omega)$	A	A	$- \ -$
-17	$\sqrt{-17}$	$-2^2 \cdot 17$	(1)	J^4	J^4	$+ \ +$
			$(3,\ 1-\sqrt{-17})$	J^3	J^2	
			$(2,\ 1+\sqrt{-17})$	J^2	J^3	$- \ -$
			$(3,\ 1+\sqrt{-17})$	J	J	
-19	$\frac{1+\sqrt{-19}}{2}$	-19	(1)	1	1	$+$
-21	$\sqrt{-21}$	$-2^2 \cdot 3 \cdot 7$	(1)	$A^2 A_1^2$	1	$+ \ + \ +$
			$(5,\ 3+\sqrt{-21})$	$A A_1$	$A A_1$	$+ \ - \ -$
			$(3,\ \sqrt{-21})$	A_1	A_1	$- \ + \ -$
			$(2,\ 1+\sqrt{-21})$	A	A	$- \ - \ +$
-22	$\sqrt{-22}$	$-2^2 \cdot 11$	(1)	A^2	A^2	$+ \ +$
			$(2,\ \sqrt{-22})$	A	A	$- \ -$
-23	$\frac{1+\sqrt{-23}}{2}$	-23	(1)	J^3	J^3	$+$
			$(2,\ \omega')$	J^2	J^2	
			$(2,\ \omega)$	J	J	
-26	$\sqrt{-26}$	$-2^2 \cdot 13$	(1)	J^6	J^6	$+ \ +$
			$(5,\ 2-\sqrt{-26})$	J^5	J^4	
			$(3,\ 1+\sqrt{-26})$	J^4	J^2	
			$(2,\ \sqrt{-26})$	J^3	J^5	$- \ -$
			$(3,\ 1-\sqrt{-26})$	J^2	J^3	
			$(5,\ 2+\sqrt{-26})$	J	J	
-29	$\sqrt{-29}$	$-2^2 \cdot 29$	(1)	J^6	J^6	$+ \ +$
			$(3,\ 1-\sqrt{-29})$	J^5	J^4	
			$(5,\ 1-\sqrt{-29})$	J^4	J^2	
			$(2,\ 1+\sqrt{-29})$	J^3	J^5	$- \ -$
			$(5,\ 1+\sqrt{-29})$	J^2	J^3	
			$(3,\ 1+\sqrt{-29})$	J	J	
-30	$\sqrt{-30}$	$-2^2 \cdot 3 \cdot 5$	(1)	$A^2 A_1^2$	$A^2 A_1^2$	$+ \ + \ +$
			$(2,\ \sqrt{-30})$	$A A_1$	$A A_1$	$+ \ - \ -$
			$(3,\ \sqrt{-30})$	A_1	A_1	$- \ + \ -$
			$(5,\ \sqrt{-30})$	A	A	$- \ - \ +$

	Base 1 ω	d	Idéaux	Classes	Genres	Systèmes de caractères
-31	$\frac{1+\sqrt{-31}}{2}$	-31	(1)	J^3	J^3	$+$
			$(2,\ 1+\omega')$	J^2	J^2	
			$(2,\ 1+\omega)$	J	J	
-33	$\sqrt{-33}$	$-2^2\cdot 3\cdot 11$	(1)	$A^2A_1{}^2$	$A^2A_1{}^2$	$+\ +\ +$
			$(2, 1+\sqrt{-33})$	AA_1	AA_1	$+\ -\ -$
			$(3,\ \sqrt{-33})$	A_1	A_1	$-\ +\ -$
			$(6, 3+\sqrt{-33})$	A	A	$-\ -\ +$
-34	$\sqrt{-34}$	$-2^3\cdot 17$	(1)	J^4	J^4	$+\ +$
			$(5, 1-\sqrt{-34})$	J^3	J^2	
			$(2,\ \sqrt{-34})$	J^2	J^3	$-\ -$
			$(5, 1+\sqrt{-34})$	J	J	
-35	$\frac{1+\sqrt{-35}}{2}$	$-5\cdot 7$	(1)	A^2	A^2	$+\ +$
			$(5,\ \sqrt{-35})$	A	A	$-\ -$
-37	$\sqrt{-37}$	$-2^2\cdot 37$	(1)	A^2	A^2	$+\ +$
			$(2, 1+\sqrt{-37})$	A	A	$-\ -$
-38	$\sqrt{-38}$	$-2^3\cdot 19$	(1)	J^6	J^6	$+\ +$
			$(3, 1-\sqrt{-38})$	J^5	J^4	
			$(7, 2+\sqrt{-38})$	J^4	J^2	
			$(2,\ \sqrt{-38})$	J^3	J^5	$-\ -$
			$(7, 2-\sqrt{-38})$	J^2	J^3	
			$(3, 1+\sqrt{-38})$	J	J	
-39	$\frac{1+\sqrt{-39}}{2}$	$-3\cdot 13$	(1)	J^4	J^4	$+\ +$
			$(2,\ \omega')$	J^3	J^2	
			$(3,\ 1-2\omega)$	J^2	J^3	$-\ -$
			$(2,\ \omega)$	J	J	
-41	$\sqrt{-41}$	$-2^2\cdot 41$	(1)	J^8	J^8	$+\ +$
			$(3, 1-\sqrt{-41})$	J^7	J^6	
			$(5, 2-\sqrt{-41})$	J^6	J^4	
			$(7, 1-\sqrt{-41})$	J^5	J^2	
			$(2, 1+\sqrt{-41})$	J^4	J^7	$-\ -$
			$(7, 1+\sqrt{-41})$	J^3	J^5	
			$(5, 2+\sqrt{-41})$	J^2	J^3	
			$(3, 1+\sqrt{-41})$	J	J	

	Base 1 ω	d	Idéaux	Classes	Genres	Systèmes de caractères
-42	$\sqrt{-42}$	$-2^3 \cdot 3 \cdot 7$	(1)	$A^2A_1^2$	$A^2A_1^2$	$+ \; + \; +$
			$(7, \sqrt{-42})$	AA_1	AA_1	$+ \; - \; -$
			$(3, \sqrt{-42})$	A_1	A_1	$- \; + \; -$
			$(2, \sqrt{-42})$	A	A	$- \; - \; +$
-43	$\frac{1+\sqrt{-43}}{2}$	-43	(1)	1	1	$+$
-46	$\sqrt{-46}$	$-2^3 \cdot 23$	(1)	J^4	J^4	$+ \; +$
			$(5, 2-\sqrt{-46})$	J^3	J^2	
			$(2, \sqrt{-46})$	J^2	J^3	$- \; -$
			$(5, 2+\sqrt{-46})$	J	J	
-47	$\frac{1+\sqrt{-47}}{2}$	-47	(1)	J^5	J^5	$+$
			$(2, 1+\omega')$	J^4	J^4	
			$(3, \omega')$	J^3	J^3	
			$(3, \omega)$	J^2	J^2	
			$(2, 1+\omega)$	J	J	
-51	$\frac{1+\sqrt{-51}}{2}$	$-3 \cdot 17$	(1)	A^2	A^2	$+ \; +$
			$(3, 1-2\omega)$	A	A	$- \; -$
-53	$\sqrt{-53}$	$-2^2 \cdot 53$	(1)	J^6	J^6	$+ \; +$
			$(3, 1-\sqrt{-53})$	J^5	J^4	
			$(9, 1-\sqrt{-53})$	J^4	J^2	
			$(2, 1+\sqrt{-53})$	J^3	J^5	$- \; -$
			$(9, 1+\sqrt{-53})$	J^2	J^3	
			$(3, 1+\sqrt{-53})$	J	J	
-55	$\frac{1+\sqrt{-55}}{2}$	$-5 \cdot 11$	(1)	J^4	J^4	$+ \; +$
			$(2, \omega')$	J^3	J	
			$(5, 1-2\omega)$	J^2	J^3	$- \; -$
			$(2, \omega)$	J	J	
-57	$\sqrt{-57}$	$-2^2 \cdot 3 \cdot 19$	(1)	$A^2A_1^2$	$A^2A_1^2$	$+ \; + \; +$
			$(2, 1+\sqrt{-57})$	AA_1	AA_1	$+ \; - \; -$
			$(3, \sqrt{-57})$	A_1	A_1	$- \; + \; -$
			$(6, 3+\sqrt{-57})$	A	A	$- \; - \; +$
-58	$\sqrt{-58}$	$-2^3 \cdot 29$	(1)	A^2	A^2	$+ \; +$
			$(2, \sqrt{-58})$	A	A	$- \; -$

	Base 1 ω		Idéaux	Classes	Genres	Systèmes de caractères
-59	$\frac{1+\sqrt{-59}}{2}$	-59	(1)	J^3	J^3	
			$(3, \omega')$	J^2	J^2	$+$
			$(3, \omega)$	J	J	
-61	$\sqrt{-61}$	$-2^2 \cdot 61$	(1)	J^3	J^3	
			$(5, 2-\sqrt{-61})$	J^2	J^2	$+ \quad +$
			$(5, 2+\sqrt{-61})$	J	J	
			$(7, 3-\sqrt{-61})$	AJ^2	AJ^2	
			$(7, 3+\sqrt{-61})$	AJ	AJ	$- \quad -$
			$(2, 1+\sqrt{-61})$	A	A	
-62	$\sqrt{-62}$	$-2^3 \cdot 31$	1	J^8	J^8	
			$(3, 1-\sqrt{-62})$	J^7	J^6	$+ \quad +$
			$(7, 1+\sqrt{-62})$	J^6	J^4	
			$(11, 2+\sqrt{-62})$	J^5	J^2	
			$(2, \sqrt{-62})$	J^4	J^7	
			$(11, 2-\sqrt{-62})$	J^3	J^5	$- \quad -$
			$(7, 1-\sqrt{-62})$	J^2	J^3	
			$(3, 1+\sqrt{-62})$	J	J	
-65	$\sqrt{-65}$	$-2^2 \cdot 5 \cdot 13$	(1)	J^4	J^4	$+ \quad + \quad +$
			$(3, 1-\sqrt{-65})$	J^3	J^2	
			$(9, 5-\sqrt{-65})$	J^2	AJ^2	$+ \quad - \quad -$
			$(3, 1+\sqrt{-65})$	J	A	
			$(11, 1-\sqrt{-65})$	AJ^3	AJ^3	$- \quad + \quad -$
			$(2, 1+\sqrt{-65})$	AJ^2	AJ	
			$(11, 1+\sqrt{-65})$	AJ	J^3	$- \quad - \quad +$
			$(5, \sqrt{-65})$	A	J	
-66	$\sqrt{-66}$	$-2^3 \cdot 3 \cdot 11$	(1)	J^4	J^4	$+ \quad + \quad +$
			$(5, 2-\sqrt{-66})$	J^3	J^2	
			$(3, \sqrt{-66})$	J^2	AJ^2	$+ \quad - \quad -$
			$(5, 2+\sqrt{-66})$	J	A	
			$(7, 2+\sqrt{-66})$	AJ^3	AJ^3	$- \quad + \quad -$
			$(11, \sqrt{-66})$	AJ^2	AJ	
			$(7, 2-\sqrt{-66})$	AJ	J^3	$- \quad - \quad +$
			$(2, \sqrt{-66})$	A	J	
-67	$\frac{1+\sqrt{-67}}{2}$	-67	(1)	1	1	$+$

	Base 1 ω	d	Idéaux	Classes	Genres	Systèmes de caractères
-86	$\sqrt{-86}$	$-2^3 \cdot 43$	$(2, \sqrt{-86})$	J^5	$J^{[illegible]}$	
			$(17, 4+\sqrt{-86})$	J^4	J^7	
			$(5, 2-\sqrt{-86})$	J^3	J^6	$-\ -$
			([illegible], $2-\sqrt{-86}$)	J^2	J^3	
			$(3, 1+\sqrt{-86})$	J	J	
-87	$\dfrac{1+\sqrt{-87}}{2}$	$-3 \cdot 29$	(1)	J^6	J^6	
			$(2, \omega')$	J^5	J^4	$+\ +$
			$(7, 2+\omega)$	J^4	J^2	
			$(3, 1+\omega)$	J^3	J^5	
			$(7, 2+\omega')$	J^2	J^3	$-\ -$
			$(2, \omega)$	J	J	
-89	$\sqrt{-89}$	$-2^2 \cdot 89$	(1)	J^{12}	J^{12}	
			$(3, 1-\sqrt{-89})$	J^{11}	J^{10}	
			$(17, 8-\sqrt{-89})$	J^{10}	J^8	
			$(7, 4-\sqrt{-89})$	J^9	J^6	$+\ +$
			$(5, 1-\sqrt{-89})$	J^8	J^4	
			$(6, 1+\sqrt{-89})$	J^7	J^2	
			$(2, 1+\sqrt{-89})$	J^6	J^{11}	
			$(6, 1-\sqrt{-89})$	J^5	J^9	
			$(5, 1+\sqrt{-89})$	J^4	J^7	
			$(7, 4+\sqrt{-89})$	J^3	J^5	$-\ -$
			$(17, 8+\sqrt{-89})$	J^2	J^3	
			$(3, 1+\sqrt{-89})$	J	J	
-91	$\dfrac{1+\sqrt{-91}}{2}$	$-7 \cdot 13$	(1)	A^2	A^2	$+\ +$
			$(7, \sqrt{-91})$	A	A	$-\ -$
-93	$\sqrt{-93}$	$-2^2 \cdot 3 \cdot 31$	(1)	$A^2 A_1^2$	$A^2 A_1^2$	$+\ +\ +$
			$(6, 3+\sqrt{-93})$	AA_1	AA_1	$+\ -\ -$
			$(3, \sqrt{-93})$	A_1	A_1	$-\ +\ -$
			$(2, 1+\sqrt{-93})$	A	A	$-\ -\ +$
-94	$\sqrt{-94}$	$-2^3 \cdot 47$	(1)	J^8	J^8	
			$(5, 1-\sqrt{-94})$	J^7	J^6	$+\ +$
			$(7, 2-\sqrt{-94})$	J^6	J^4	
			$(11, 4+\sqrt{-94})$	J^5	J^2	

	Base 1, ω	d	Idéaux	Classes	Genres	Systèmes de caractères
−69	$\sqrt{-69}$	$-2^2\cdot 3\cdot 23$	(1)	J^4	J^4	+ + +
			$(7, 1-\sqrt{-69})$	J^3	J^2	
			$(6, 3+\sqrt{-69})$	J^2	AJ^3	+ − −
			$(7, 1+\sqrt{-69})$	J	AJ	
			$(5, 1+\sqrt{-69})$	AJ^3	J^3	− + −
			$(3, \sqrt{-69})$	AJ^2	J	
			$(5, 1-\sqrt{-69})$	AJ	AJ^2	− − +
			$(2, 1+\sqrt{-69})$	A	A	
−70	$\sqrt{-70}$	$-2^3\cdot 5\cdot 7$	(1)	$A^2A_1^2$	$A^2A_1^2$	+ + +
			$(7, \sqrt{-70})$	AA_1	AA_1	+ − −
			$(5, \sqrt{-70})$	A_1	A_1	− + −
			$(2, \sqrt{-70})$	A	A	− − +
−71	$\frac{1+\sqrt{-71}}{2}$	−71	(1)	J^7	J^7	+
			$(2, \omega')$	J^6	J^6	
			$(5, 1+\omega')$	J^5	J^5	
			$(3, 2+\omega)$	J^4	J^4	
			$(3, 2+\omega')$	J^3	J^3	
			$(5, 1+\omega)$	J^2	J^2	
			$(2, \omega)$	J	J	
−73	$\sqrt{-73}$	$-2^2\cdot 73$	(1)	J^4	J^4	+ +
			$(7, 2-\sqrt{-73})$	J^3	J^2	
			$(2, 1+\sqrt{-73})$	J^2	J^3	− −
			$(7, 2+\sqrt{-73})$	J	J	
−74	$\sqrt{-74}$	$-2^3\cdot 37$	(1)	J^5	J^5	+ +
			$(11, 5-\sqrt{-74})$	J^4	J^4	
			$(3, 1-\sqrt{-74})$	J^3	J^3	
			$(3, 1+\sqrt{-74})$	J^2	J^2	
			$(11, 5+\sqrt{-74})$	J	J	
			$(5, 1-\sqrt{-74})$	AJ^4	AJ^4	− −
			$(6, 2+\sqrt{-74})$	AJ^3	AJ^3	
			$(6, 2-\sqrt{-74})$	AJ^2	AJ^2	
			$(5, 1+\sqrt{-74})$	AJ	AJ	
			$(2, \sqrt{-74})$	A	A	

	Base 1 ω	d	Idéaux	Classes	Genres	Systèmes de caractères
-77	$\sqrt{-77}$	$-2^2\cdot 7\cdot 11$	(1)	J^4	J^4	$+\ +\ +$
			$(3, 1-\sqrt{-77})$	J^3	J^2	
			$(14, 7+\sqrt{-77})$	J^2	AJ^3	$+\ -\ -$
			$(3, 1+\sqrt{-77})$	J	AJ	
			$(6, 1-\sqrt{-77})$	AJ^3	AJ^2	$-\ +\ -$
			$(7, \sqrt{-77})$	AJ^2	A	
			$(6, 1+\sqrt{-77})$	AJ	J^3	$-\ -\ +$
			$(2, 1+\sqrt{-77})$	A	J	
-78	$\sqrt{-78}$	$-2^3\cdot 3\cdot 13$	(1)	$A^2A_1{}^2$	$A^2A_1{}^2$	$+\ +\ +$
			$(2, \sqrt{-78})$	AA_1	AA_1	$+\ -\ -$
			$(13, \sqrt{-78})$	A_1	A_1	$-\ +\ -$
			$(3, \sqrt{-78})$	A	A	$-\ -\ +$
-79	$\dfrac{1+\sqrt{-79}}{2}$	-79	(1)	J^5	J^5	$+$
			$(2, 1+\omega')$	J^4	J^4	
			$(5, \omega')$	J^3	J^3	
			$(5, \omega)$	J^2	J^2	
			$(2, 1+\omega)$	J	J	
-82	$\sqrt{-82}$	$-2^3\cdot 41$	(1)	J^4	J^4	$+\ +$
			$(7, 3-\sqrt{-82})$	J^3	J^2	
			$(2, \sqrt{-82})$	J^2	J^3	$-\ -$
			$(7, 3+\sqrt{-82})$	J	J	
83	$\dfrac{1+\sqrt{-83}}{2}$	-83	(1)	J^3	J^3	$+$
			$(3, \omega')$	J^2	J^2	
			$(3, \omega)$	J	J	
-85	$\sqrt{-85}$	$-2^2\cdot 5\cdot 17$	(1)	$A^2A_1{}^2$	$A^2A_1{}^2$	$+\ +\ +$
			$(5, \sqrt{-85})$	AA_1	AA_1	$+\ -\ -$
			$(10, 5+\sqrt{-85})$	A_1	A_1	$-\ +\ -$
			$(2, 1+\sqrt{-85})$	A	A	$-\ -\ +$
-86	$\sqrt{-86}$	$-2^3\cdot 43$	(1)	J^{10}	J^{10}	$+\ +$
			$(3, 1-\sqrt{-86})$	J^9	J^8	
			$(9, 2+\sqrt{-86})$	J^8	J^6	
			$(5, 2+\sqrt{-86})$	J^7	J^4	
			$(17, 4-\sqrt{-86})$	J^6	J^2	

	Base 1 ω	d	Idéaux	Classes	Genres	Systèmes de caractères
— 94	$\sqrt{-94}$	$-2^3 \cdot 47$	$(2, \sqrt{-94})$	J^4	J^7	$-\ -$
			$(11, 4-\sqrt{-94})$	J^3	J^5	
			$(7, 2+\sqrt{-94})$	J^2	J^3	
			$(5, 1+\sqrt{-94})$	J	J	
— 95	$\frac{1+\sqrt{-95}}{2}$	$-5 \cdot 19$	(1)	J^8	J^8	$+\ +$
			$(2, 1+\omega')$	J^7	J^6	
			$(4, 1-\omega')$	J^6	J^4	
			$(3, \omega')$	J^5	J^2	
			$(5, 1-2\omega)$	J^4	J^7	$-\ -$
			$(3, \omega)$	J^3	J^5	
			$(4, 1-\omega)$	J^2	J^3	
			$(2, 1+\omega)$	J	J	
— 97	$\sqrt{-97}$	$-2^2 \cdot 97$	(1)	J^4	J^4	$+\ +$
			$(7, 1-\sqrt{-97})$	J^3	J^2	
			$(2, 1+\sqrt{-97})$	J^2	J^3	$-\ -$
			$(7, 1+\sqrt{-97})$	J	J	

CORPS RÉELS

	Base 1, ω	d	ε	$n(\varepsilon)$	Idéaux	Classes	Genres	Systèmes de caractères
2	$\sqrt{2}$	2^3	$1+\sqrt{2}$	-1	(1)	1	1	$+$
3	$\sqrt{3}$	$3 \cdot 2^2$	$2+\sqrt{3}$	$+1$	(1)	1	1	$+$
5	$\frac{1+\sqrt{5}}{2}$	5	ω	-1	(1)	1	1	$+$
6	$\sqrt{6}$	$3 \cdot 2^3$	$5+2\sqrt{6}$	$+1$	(1)	1	1	$+$
7	$\sqrt{7}$	$7 \cdot 2^2$	$8+3\sqrt{7}$	$+1$	(1)	1	1	$+$
10	$\sqrt{10}$	$2^3 \cdot 5$	$3+\sqrt{10}$	-1	(1) $(2, \sqrt{10})$	A^2 A	A^2 A	$+\ +$ $-\ -$
11	$\sqrt{11}$	$11 \cdot 2^2$	$10+3\sqrt{11}$	$+1$	(1)	1	1	$+$
13	$\frac{1+\sqrt{13}}{2}$	13	$1+\omega$	-1	(1)	1	1	$+$
14	$\sqrt{14}$	$7 \cdot 2^3$	$15+4\sqrt{14}$	$+1$	(1)	1	1	$+$
15	$\sqrt{15}$	$3 \cdot 2^2 \cdot 5$	$4+\sqrt{15}$	$+1$	(1) $(2, 1+\sqrt{15})$	A^2 A	A^2 A	$+\ +$ $-\ -$
17	$\frac{1+\sqrt{17}}{2}$	17	$3+2\omega$	-1	(1)	1	1	$+$
19	$\sqrt{19}$	$19 \cdot 2^2$	$170+39\sqrt{19}$	$+1$	(1)	1	1	$+$
21	$\frac{1+\sqrt{21}}{2}$	$3 \cdot 7$	$2+\omega$	$+1$	(1)	1	1	$+$
22	$\sqrt{22}$	$11 \cdot 2^3$	$197+42\sqrt{22}$	$+1$	(1)	1	1	$+$
23	$\sqrt{23}$	$23 \cdot 2^2$	$24+5\sqrt{23}$	$+1$	(1)	1	1	$+$

	Base : 1, ω	d	ε	n(ε)	Idéaux	Classes	Genres	Systèmes de caractères
26	$\sqrt{26}$	$2^3 \cdot 13$	$5 + \sqrt{26}$	-1	(1) $(2, \sqrt{26})$	A^2 A	A^2 A	+ + − −
29	$\frac{1 + \sqrt{29}}{2}$	29	$2 + \omega$	-1	(1)	1	1	+
30	$\sqrt{30}$	$3 \cdot 2^3 \cdot 5$	$11 + 2\sqrt{30}$	$+1$	(1) $(2, \sqrt{30})$	A^2 A	A^2 A	+ + − −
31	$\sqrt{31}$	$31 \cdot 2^2$	$1520 + 273\sqrt{31}$	$+1$	(1) $(3, 1 - \sqrt{-31})$ $(3, 1 + \sqrt{-31})$	J^3 J^2 J	J^3 J^2 J	+
33	$\frac{1 + \sqrt{33}}{2}$	$3 \cdot 11$	$19 + 8\omega$	$+1$	(1)	1	1	+
34*	$\sqrt{34}$	$2^3 \cdot 17$	$35 + 6\sqrt{34}$	$+1$	(1) $(3, 1 + \sqrt{34})$	A^2 A	A^2 A	+ + − −
35	$\sqrt{35}$	$7 \cdot 2^2 \cdot 5$	$6 + \sqrt{35}$	$+1$	(1) $(2, 1 + \sqrt{35})$	A^2 A	A^2 A	+ + − −
37	$\frac{1 + \sqrt{37}}{2}$	37	$5 + 2\omega$	-1	(1)	1	1	+
38	$\sqrt{38}$	$19 \cdot 2^3$	$37 + 6\sqrt{38}$	$+1$	(1)	1	1	+
39	$\sqrt{39}$	$3 \cdot 2^2 \cdot 13$	$25 + 4\sqrt{39}$	$+1$	(1) $(2, 1 + \sqrt{39})$	A^2 A	A^2 A	+ + − −
41	$\frac{1 + \sqrt{41}}{2}$	41	$27 + 10\omega$	-1	(1)	1	1	+
42	$\sqrt{42}$	$3 \cdot 2^3 \cdot 7$	$13 + 2\sqrt{42}$	$+1$	(1) $(2, \sqrt{42})$	A^2 A	A^2 A	+ + − −
43	$\sqrt{43}$	$43 \cdot 2^2$	$3482 + 531\sqrt{43}$	$+1$	(1)	1	1	+
46	$\sqrt{46}$	$23 \cdot 2^3$	$24335 + 3588\sqrt{46}$	$+1$	(1)	1	1	+
47	$\sqrt{47}$	$47 \cdot 2^2$	$48 + 7\sqrt{47}$	$+1$	(1)	1	1	+

	Base 1, ω	d	ε	$n(\varepsilon)$	Idéaux	Classes	Genres	Systèmes de caractères
77	$\frac{1+\sqrt{77}}{2}$	$7 \cdot 11$	$4 + \omega$	$+1$	(1)	1	1	$+$
78	$\sqrt{78}$	$3 \cdot 2^3 \cdot 13$	$53 + 6\sqrt{78}$	$+1$	(1) $(2, \sqrt{78})$	A^2 A	A^2 A	$+\ +$ $-\ -$
79	$\sqrt{79}$	$79 \cdot 2^2$	$80 + 9\sqrt{79}$	$+1$	(1) $(3, 1-\sqrt{79})$ $(3, 1+\sqrt{79})$	J^3 J^2 J	J^3 J^2 J	$+$
82	$\sqrt{82}$	$2^3 \cdot 41$	$9 + \sqrt{82}$	-1	(1) $(3, 2-\sqrt{82})$ $(2, \sqrt{82})$ $(5, 2+\sqrt{82})$	J^4 J^3 J^2 J	J^4 J^2 J^3 J	$+\ +$ $-\ -$
83	$\sqrt{83}$	$83 \cdot 2^2$	$82 + 9\sqrt{83}$	$+1$	(1)	1	1	$+$
85	$\frac{1+\sqrt{85}}{2}$	$5 \cdot 17$	$4 + \omega$	-1	(1) $(5, \sqrt{85})$	A^2 A	A^2 A	$+\ +$ $-\ -$
86	$\sqrt{86}$	$43 \cdot 2^3$	$10405 + 1122\sqrt{86}$	$+1$	(1)	1	1	$+$
87	$\sqrt{87}$	$3 \cdot 2^2 \cdot 29$	$28 + 3\sqrt{87}$	$+1$	(1) $(2, 1+\sqrt{87})$	A^2 A	A^2 A	$+\ +$ $-\ -$
89	$\frac{1+\sqrt{89}}{2}$	89	$447 + 106\,\omega$	-1	(1)	1	1	$+$
91	$\sqrt{91}$	$7 \cdot 2^2 \cdot 13$	$1574 + 165\sqrt{91}$	$+1$	(1) $(2, 1+\sqrt{91})$	A^2 A	A^2 A	$+\ +$ $-\ -$
93	$\frac{1+\sqrt{93}}{2}$	$3 \cdot 31$	$13 + 3\,\omega$	$+1$	(1)	1	1	$+$
94	$\sqrt{94}$	$47 \cdot 2^3$	$2143295 +$ $221064\sqrt{94}$	$+1$	(1)	1	1	$+$
95	$\sqrt{95}$	$19 \cdot 2^2 \cdot 5$	$39 + 4\sqrt{95}$	$+1$	(1) $(2, 1+\sqrt{95})$	A^2 A	A^2 A	$+\ +$ $-\ -$
97	$\frac{1+\sqrt{97}}{2}$	97	$5035 + 1138\,\omega$	-1	(1)	1	1	$+$
101	$\frac{1+\sqrt{101}}{2}$	101	$9 + 2\,\omega$	-1	(1)	1	1	$+$

	Base 1, ω	d	ε	$n(\varepsilon)$	Idéaux	Classes	Genres	Systèmes de caractères
51	$\sqrt{51}$	$3 \cdot 2^2 \cdot 17$	$50 + 7\sqrt{51}$	$+1$	(1) $(3, \sqrt{51})$	A^2 A	A^2 A	$+\ +$ $-\ -$
53	$\frac{1+\sqrt{53}}{2}$	53	$3 + \omega$	-1	(1)	1	1	$+$
55	$\sqrt{55}$	$11 \cdot 2^2 \cdot 5$	$89 + 12\sqrt{55}$	$+1$	(1) $(2, 1+\sqrt{55})$	A^2 A	A^2 A	$+\ +$ $-\ -$
57	$\frac{1+\sqrt{57}}{2}$	$3 \cdot 19$	$131 + 40\omega$	$+1$	(1)	1	1	$+$
58	$\sqrt{58}$	$2^3 \cdot 29$	$99 + 13\sqrt{58}$	-1	(1) $(2, \sqrt{58})$	A^2 A	A^2 A	$+\ +$ $-\ -$
59	$\sqrt{59}$	$59 \cdot 2^2$	$530 + 69\sqrt{59}$	$+1$	(1)	1	1	$+$
61	$\frac{1+\sqrt{61}}{2}$	61	$17 + 5\omega$	-1	(1)	1	1	$+$
62	$\sqrt{62}$	$31 \cdot 2^3$	$63 + 8\sqrt{62}$	$+1$	(1)	1	1	$+$
65	$\frac{1+\sqrt{65}}{2}$	$5 \cdot 13$	$7 + 2\omega$	-1	(1) $(5, \sqrt{65})$	A^2 A	A^2 A	$+\ +$ $-\ -$
66	$\sqrt{66}$	$3 \cdot 2^3 \cdot 11$	$65 + 8\sqrt{66}$	$+1$	(1) $(3, \sqrt{66})$	A^2 A	A^2 A	$+\ +$ $-\ -$
67	$\sqrt{67}$	$67 \cdot 2^2$	$48842 + 5967\sqrt{67}$	$+1$	(1)	1	1	$+$
69	$\frac{1+\sqrt{69}}{2}$	$3 \cdot 23$	$11 + 3\omega$	$+1$	(1)	1	1	$+$
70	$\sqrt{70}$	$7 \cdot 2^3 \cdot 5$	$251 + 30\sqrt{70}$	$+1$	(1) $(2, \sqrt{70})$	A^2 A	A^2 A	$+\ +$ $-\ -$
71	$\sqrt{71}$	$71 \cdot 2^2$	$3480 + 413\sqrt{71}$	$+1$	(1)	1	1	$+$
73	$\frac{1+\sqrt{73}}{2}$	73	$943 + 250\omega$	-1	(1)	1	1	$+$
74	$\sqrt{74}$	$2^3 \cdot 37$	$43 + 5\sqrt{74}$	-1	(1) $(2, \sqrt{74})$	A^2 A	A^2 A	$+\ +$ $-\ -$

TABLE DES MATIÈRES

CHAPITRE PREMIER

INTRODUCTION

CHAPITRE II

LE CORPS QUADRATIQUE

CHAPITRE III

APPLICATIONS DE LA THÉORIE DU CORPS QUADRATIQUE

CHAPITRE IV

LES CORPS DU TROISIÈME DEGRÉ

CHAPITRE V

LE CORPS RELATIF

Saint-Amand, Cher. — Imprimerie A. Bussière.

